

John J. Nelson (SBN 317598)  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, LLC**  
280 S. Beverly Drive  
Beverly Hills, CA 90212  
Telephone: (858) 209-6941  
Email: jnelson@milberg.com

*Attorney for Plaintiff and the Proposed Class*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

LYNSEY SAURENMANN, on behalf of  
herself and all others similarly situated,

Plaintiff,

v.

CITY OF HOPE,

Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION**

**DEMAND FOR A JURY TRIAL**

Plaintiff Lynsey Saurenmann ("Plaintiff") brings this Class Action Complaint ("Complaint") against City of Hope ("Hope" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

**SUMMARY OF ACTION**

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information of its patients.

1           2. Defendant is a cancer research, treatment, and prevention company that  
2 provides healthcare services for “patients across the United States through [its]  
3 national footprint of cancer centers.”<sup>1</sup>  
4

5           3. Plaintiff’s and Class Members’ sensitive personal information—which  
6 they entrusted to Defendant on the mutual understanding that Defendant would  
7 protect it against disclosure—was targeted, compromised and unlawfully accessed  
8 due to the Data Breach.  
9

10           4. Hope collected and maintained certain personally identifiable  
11 information and protected health information of Plaintiff and the putative Class  
12 Members (defined below), who are (or were) patients at Defendant.  
13

14           5. The Private Information compromised in the Data Breach included  
15 Plaintiff’s and Class Members’ full names, contact information, dates of birth,  
16 driver’s licenses or government identifications, financial details, and Social Security  
17 numbers (“personally identifiable information” or “PII”) and medical treatment and  
18 health insurance information, which is protected health information (“PHI,” and  
19 collectively with PII, “Private Information”) as defined by the Health Insurance  
20 Portability and Accountability Act of 1996 (“HIPAA”).  
21  
22  
23  
24  
25  
26

---

27 <sup>1</sup> <https://www.cityofhope.org/>  
28

1           6.     The Private Information compromised in the Data Breach was  
2     exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who  
3  
4     target Private Information for its value to identity thieves.

5           7.     As a result of the Data Breach, Plaintiff and approximately 827,000  
6     Class Members,<sup>2</sup> suffered concrete injuries in fact including, but not limited to: (i)  
7  
8     invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished  
9     value of Private Information; (iv) lost time and opportunity costs associated with  
10    attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit  
11  
12   of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the  
13   actual consequences of the Data Breach; (vii) actual misuse of the compromised data  
14   consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private  
15   Information being disseminated on the dark web, according to Experian and Credit  
16  
17   Karma; (ix) statutory damages; (x) nominal damages; and (xi) the continued and  
18  
19   certainly increased risk to their Private Information, which: (a) remains unencrypted  
20   and available for unauthorized third parties to access and abuse; and (b) remains  
21   backed up in Defendant's possession and is subject to further unauthorized  
22   disclosures so long as Defendant fails to undertake appropriate and adequate  
23  
24   measures to protect the Private Information.

---

25  
26  
27   <sup>2</sup> [https://apps.web.maine.gov/online/aeviewer/ME/40/e86f6a2d-d729-49a3-83b0-  
28   f9c46afa5b9b.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/e86f6a2d-d729-49a3-83b0-f9c46afa5b9b.shtml)

1           8.     The Data Breach was a direct result of Defendant's failure to implement  
2 adequate and reasonable cyber-security procedures and protocols necessary to  
3 protect patients' Private Information from a foreseeable and preventable cyber-  
4 attack.  
5

6           9.     Moreover, upon information and belief, Defendant was targeted for a  
7 cyber-attack due to its status as a healthcare entity that collects and maintains highly  
8 valuable Private Information on its systems.  
9

10          10.    Defendant maintained, used, and shared the Private Information in a  
11 reckless manner. In particular, the Private Information was used and transmitted by  
12 Defendant in a condition vulnerable to cyberattacks. Upon information and belief,  
13 the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's  
14 and Class Members' Private Information was a known risk to Defendant, and thus,  
15 Defendant was on notice that failing to take steps necessary to secure the Private  
16 Information from those risks left that property in a dangerous condition.  
17  
18

19          11.    Defendant disregarded the rights of Plaintiff and Class Members by,  
20 *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate  
21 and reasonable measures to ensure its data systems were protected against  
22 unauthorized intrusions; failing to take standard and reasonably available steps to  
23 prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt  
24 and accurate notice of the Data Breach.  
25  
26  
27  
28

1           12. Plaintiff's and Class Members' identities are now at risk because of  
2 Defendant's negligent conduct because the Private Information that Defendant  
3 collected and maintained has been accessed and acquired by data thieves.  
4

5           13. Armed with the Private Information accessed in the Data Breach, data  
6 thieves have already engaged in identity theft and fraud and can in the future commit  
7 a variety of crimes including, *e.g.*, opening new financial accounts in Class  
8 Members' names, taking out loans in Class Members' names, using Class Members'  
9 information to obtain government benefits, filing fraudulent tax returns using Class  
10 Members' information, obtaining driver's licenses in Class Members' names but  
11 with another person's photograph, and giving false information to police during an  
12 arrest.  
13  
14  
15

16           14. As a result of the Data Breach, Plaintiff and Class Members have been  
17 exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and  
18 Class Members must now and in the future closely monitor their financial accounts  
19 to guard against identity theft.  
20

21           15. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*,  
22 for purchasing credit monitoring services, credit freezes, credit reports, or other  
23 protective measures to deter and detect identity theft.  
24

25           16. Plaintiff brings this class action lawsuit on behalf all those similarly  
26 situated to address Defendant's inadequate safeguarding of Class Members' Private  
27  
28

1 Information that it collected and maintained, and for failing to provide timely and  
2 adequate notice to Plaintiff and other Class Members that their information had been  
3 subject to the unauthorized access by an unknown third party and precisely what  
4 specific type of information was accessed.  
5

6 17. Through this Complaint, Plaintiff seeks to remedy these harms on  
7 behalf of herself and all similarly situated individuals whose Private Information  
8 was accessed during the Data Breach.  
9

10 18. Plaintiff and Class Members have a continuing interest in ensuring that  
11 their information is and remains safe, and they should be entitled to injunctive and  
12 other equitable relief.  
13

#### 14 **JURISDICTION AND VENUE**

15 19. This Court has subject matter jurisdiction over this action under 28  
16 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy  
17 exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are  
18 more than 100 members in the proposed class, and at least one member of the class  
19 is a citizen of a state different from Defendant.<sup>3</sup>  
20  
21  
22  
23  
24

---

25  
26 <sup>3</sup> According to the breach report submitted to the Office of the Maine Attorney General, 166  
27 Maine residents were impacted in the Data Breach. *See*  
28 <https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml>



1           26. In the course of their relationship, patients, including Plaintiff and Class  
2 Members, provided Defendant with at least the following: names, dates of birth,  
3 contact information, health insurance information, Social Security numbers, and  
4 other sensitive information.  
5

6           27. Upon information and belief, in the course of collecting Private  
7 Information from patients, including Plaintiff, Defendant promised to provide  
8 confidentiality and adequate security for the data it collected from patients through  
9 its applicable privacy policy and through other disclosures in compliance with  
10 statutory privacy requirements.  
11

12           28. Indeed, Defendant provides on its website that: “[w]e are required by  
13 law to maintain the privacy of your protected health information ("PHI"), to provide  
14 you with notice of our legal duties and privacy practices with respect to your PHI,  
15 and to notify you in the event of a breach of your unsecured PHI.”<sup>5</sup>  
16  
17

18           29. Plaintiff and the Class Members, as patients at Defendant, relied on  
19 these promises and on this sophisticated business entity to keep their sensitive  
20 Private Information confidential and securely maintained, to use this information for  
21 business purposes only, and to make only authorized disclosures of this information.  
22 Patients, in general, demand security to safeguard their Private Information,  
23  
24  
25

---

26  
27 <sup>5</sup> [https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023\\_English.pdf](https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023_English.pdf)  
28



1 especially when their Social Security numbers and other sensitive Private  
2 Information is involved.

### 3 4 ***The Data Breach***

5 30. On or about April 2, 2024, Defendant began sending Plaintiff and other  
6 Data Breach victims a Notice of Data Breach letter (the "Notice Letter"), informing  
7 them that:  
8

#### 9 ***What Happened?***

10 On or about October 13, 2023, City of Hope became aware of suspicious  
11 activity on a subset of its systems and immediately instituted mitigation  
12 measures to minimize any disruption to its operations. City of Hope launched  
13 an investigation into the nature and scope of the incident with the assistance  
14 of a leading cybersecurity firm, which determined that an unauthorized third  
15 party accessed a subset of our systems and obtained copies of some files  
16 between September 19, 2023, and October 12, 2023. City of Hope has  
undertaken a detailed review of the copied files to determine the incident's  
impact and has determined that some of these files may have contained your  
information.

#### 17 ***What Information Is Involved?***

18 While the investigation remains ongoing, the impacted personal information  
19 identified thus far varies by individual but may have included name, contact  
20 information (e.g., email address, phone number), date of birth, social security  
21 number, driver's license or other government identification, financial details  
22 (e.g., bank account number and/or credit card details), health insurance  
23 information, medical records and information about medical history and/or  
24 associated conditions, and/ or unique identifiers to associate individuals with  
25 City of Hope (e.g., medical record number).<sup>6</sup>

---

26 <sup>6</sup> The "Notice Letter". A sample copy is available at  
27 [https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-](https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml)  
28 [28ef738a0bf6.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml)

1           31. Omitted from the Notice Letter were the identity of the cybercriminals  
2 who perpetrated this Data Breach, the details of the root cause of the Data Breach,  
3 the vulnerabilities exploited, and the remedial measures undertaken to ensure such a  
4 breach does not occur again. To date, these omitted details have not been explained  
5 or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring  
6 that their Private Information remains protected.  
7

8  
9           32. This “disclosure” amounts to no real disclosure at all, as it fails to  
10 inform, with any degree of specificity, Plaintiff and Class Members of the Data  
11 Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability  
12 to mitigate the harms resulting from the Data Breach is severely diminished.  
13

14           33. Despite Defendant’s intentional opacity about the root cause of this  
15 incident, several facts may be gleaned from the Notice Letter, including: a) that this  
16 Data Breach was the work of cybercriminals; b) that the cybercriminals first  
17 infiltrated Defendant’s networks and systems, and downloaded data from the  
18 networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and  
19 c) that once inside Defendant’s networks and systems, the cybercriminals targeted  
20 information including Plaintiff’s and Class Members’ Social Security numbers, PHI,  
21 and other sensitive information for download and theft.  
22  
23  
24

25           34. In the context of notice of data breach letters of this type, Defendant’s  
26 use of the phrase “may have contained” is misleading lawyer language. Companies  
27  
28

1 only send notice letters because data breach notification laws require them to do so.  
2 And such letters are only sent to those persons who Defendant itself has has a  
3 reasonable belief that such personal information was accessed or acquired by an  
4 unauthorized individual or entity. Defendant cannot hide behind legalese – by  
5 sending a notice of data breach letter to Plaintiff and Class Members, it admits that  
6 Defendant itself has a reasonable belief that Plaintiff’s and Class Members’ names,  
7 Social Security numbers, PHI, and other sensitive information was accessed or  
8 acquired by an “unknown actor” – aka cybercriminals.  
9  
10  
11

12 35. Moreover, in its Notice Letter, Defendant failed to specify whether it  
13 undertook any efforts to contact the approximate 827,000 Class Members whose  
14 data was accessed and acquired in the Data Breach to inquire whether any of the  
15 Class Members suffered misuse of their data or whether Defendant was interested in  
16 hearing about misuse of their data or set up a mechanism for Class Members to report  
17 misuse of their data.  
18  
19

20 36. Defendant had obligations created by the FTC Act, HIPAA, contract,  
21 common law, and industry standards to keep Plaintiff’s and Class Members’ Private  
22 Information confidential and to protect it from unauthorized access and disclosure.  
23

24 37. Defendant did not use reasonable security procedures and practices  
25 appropriate to the nature of the sensitive information they were maintaining for  
26  
27  
28

1 Plaintiff and Class Members, causing the exposure of Private Information, such as  
2 encrypting the information or deleting it when it is no longer needed.  
3

4 38. The attacker accessed and acquired files Defendant shared with a third  
5 party containing unencrypted Private Information of Plaintiff and Class Members.  
6 Plaintiff's and Class Members' Private Information was accessed and stolen in the  
7 Data Breach.  
8

9 39. Plaintiff has been informed by Credit Karma and Experian that her  
10 Private Information has been disseminated on the dark web, and Plaintiff further  
11 believes that the Private Information of Class Members was subsequently sold on  
12 the dark web following the Data Breach, as that is the *modus operandi* of  
13 cybercriminals that commit cyber-attacks of this type.  
14  
15

16 ***Data Breaches Are Preventable***

17 40. Defendant did not use reasonable security procedures and practices  
18 appropriate to the nature of the sensitive information they were maintaining for  
19 Plaintiff and Class Members, causing the exposure of Private Information, such as  
20 encrypting the information or deleting it when it is no longer needed.  
21

22 41. Defendant could have prevented this Data Breach by, among other  
23 things, properly encrypting or otherwise protecting their equipment and computer  
24 files containing Private Information.  
25  
26  
27  
28

1       42. As explained by the Federal Bureau of Investigation, “[p]revention is  
2 the most effective defense against ransomware and it is critical to take precautions  
3 for protection.”<sup>7</sup>  
4

5       43. To prevent and detect cyber-attacks and/or ransomware attacks,  
6 Defendant could and should have implemented, as recommended by the United  
7 States Government, the following measures:  
8

- 9       • Implement an awareness and training program. Because end users are  
10 targets, employees and individuals should be aware of the threat of  
11 ransomware and how it is delivered.
- 12       • Enable strong spam filters to prevent phishing emails from reaching the  
13 end users and authenticate inbound email using technologies like Sender  
14 Policy Framework (SPF), Domain Message Authentication Reporting and  
15 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to  
16 prevent email spoofing.
- 17       • Scan all incoming and outgoing emails to detect threats and filter  
18 executable files from reaching end users.
- 19       • Configure firewalls to block access to known malicious IP addresses.
- 20       • Patch operating systems, software, and firmware on devices. Consider  
21 using a centralized patch management system.
- 22       • Set anti-virus and anti-malware programs to conduct regular scans  
23 automatically.
- 24       • Manage the use of privileged accounts based on the principle of least  
25 privilege: no users should be assigned administrative access unless  
26 absolutely needed; and those with a need for administrator accounts should  
27 only use them when necessary.

---

27       <sup>7</sup> How to Protect Your Networks from RANSOMWARE, at 3, *available at*:  
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- 1 • Configure access controls—including file, directory, and network share
- 2 permissions—with least privilege in mind. If a user only needs to read
- 3 specific files, the user should not have write access to those files,
- 4 directories, or shares.
- 5 • Disable macro scripts from office files transmitted via email. Consider
- 6 using Office Viewer software to open Microsoft Office files transmitted
- 7 via email instead of full office suite applications.
- 8 • Implement Software Restriction Policies (SRP) or other controls to prevent
- 9 programs from executing from common ransomware locations, such as
- 10 temporary folders supporting popular Internet browsers or
- 11 compression/decompression programs, including the
- 12 AppData/LocalAppData folder.
- 13 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 14 • Use application whitelisting, which only allows systems to execute
- 15 programs known and permitted by security policy.
- 16 • Execute operating system environments or specific programs in a
- 17 virtualized environment.
- 18 • Categorize data based on organizational value and implement physical and
- 19 logical separation of networks and data for different organizational units.<sup>8</sup>

20 44. To prevent and detect cyber-attacks or ransomware attacks, Defendant

21 could and should have implemented, as recommended by the Microsoft Threat

22 Protection Intelligence Team, the following measures:

23 **Secure internet-facing assets**

- 24 - Apply latest security updates
- 25 - Use threat and vulnerability management
- 26 - Perform regular audit; remove privileged credentials;

---

27 <sup>8</sup> *Id.* at 3-4.

1           **Thoroughly investigate and remediate alerts**

- 2           -       Prioritize and treat commodity malware infections as potential  
3                   full compromise;

4           **Include IT Pros in security discussions**

- 5           -       Ensure collaboration among [security operations], [security  
6                   admins], and [information technology] admins to configure  
7                   servers and other endpoints securely;

8           **Build credential hygiene**

- 9           -       Use [multifactor authentication] or [network level authentication]  
10                   and use strong, randomized, just-in-time local admin passwords;

11           **Apply principle of least-privilege**

- 12           -       Monitor for adversarial activities  
13           -       Hunt for brute force attempts  
14           -       Monitor for cleanup of Event Logs  
15           -       Analyze logon events;

16           **Harden infrastructure**

- 17           -       Use Windows Defender Firewall  
18           -       Enable tamper protection  
19           -       Enable cloud-delivered protection  
20           -       Turn on attack surface reduction rules and [Antimalware Scan  
21                   Interface] for Office [Visual Basic for Applications].<sup>9</sup>

22  
23  
24  
25  
26           <sup>9</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:*  
27           [https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)  
28           [preventable-disaster/](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)

1           45. Given that Defendant was storing the Private Information of its current  
2 and former patients, Defendant could and should have implemented all of the above  
3 measures to prevent and detect cyberattacks.  
4

5           46. The occurrence of the Data Breach indicates that Defendant failed to  
6 adequately implement one or more of the above measures to prevent cyberattacks,  
7 resulting in the Data Breach and data thieves acquiring and accessing the Private  
8 Information of more than eight hundred thousand individuals, including that of  
9 Plaintiff and Class Members.  
10

11           ***Defendant Acquires, Collects, And Stores Its Patients' Private Information***  
12

13           47. Defendant acquires, collects, and stores a massive amount of Private  
14 Information on its current and former patients.  
15

16           48. As a condition of obtaining healthcare services at Defendant, Defendant  
17 requires that patients and other personnel entrust it with highly sensitive personal  
18 information.  
19

20           49. By obtaining, collecting, and using Plaintiff's and Class Members'  
21 Private Information, Defendant assumed legal and equitable duties and knew or  
22 should have known that it was responsible for protecting Plaintiff's and Class  
23 Members' Private Information from disclosure.  
24



1           50. Plaintiff and the Class Members have taken reasonable steps to  
2 maintain the confidentiality of their Private Information and would not have  
3 entrusted it to Defendant absent a promise to safeguard that information.  
4

5           51. Upon information and belief, in the course of collecting Private  
6 Information from patients, including Plaintiff, Defendant promised to provide  
7 confidentiality and adequate security for their data through its applicable privacy  
8 policy and through other disclosures in compliance with statutory privacy  
9 requirements.  
10

11           52. Indeed, Defendant provides on its website that: “[w]e are required by  
12 law to maintain the privacy of your protected health information ("PHI"), to provide  
13 you with notice of our legal duties and privacy practices with respect to your PHI,  
14 and to notify you in the event of a breach of your unsecured PHI.”<sup>10</sup>  
15  
16

17           53. Plaintiff and the Class Members relied on Defendant to keep their  
18 Private Information confidential and securely maintained, to use this information for  
19 business purposes only, and to make only authorized disclosures of this information.  
20  
21  
22  
23  
24  
25  
26

---

27 <sup>10</sup> [https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023\\_English.pdf](https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023_English.pdf)  
28

***Defendant Knew, Or Should Have Known, of the Risk Because Healthcare Entities In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks***

54. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

55. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

56. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>11</sup>

57. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

<sup>11</sup> See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

1           58. Indeed, cyber-attacks, such as the one experienced by Defendant, have  
2 become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S.  
3 Secret Service have issued a warning to potential targets so they are aware of, and  
4 prepared for, a potential attack. As one report explained, smaller entities that store  
5 Private Information are “attractive to ransomware criminals...because they often  
6 have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>12</sup>  
7  
8

9           59. Additionally, as companies became more dependent on computer  
10 systems to run their business,<sup>13</sup> e.g., working remotely as a result of the Covid-19  
11 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is  
12 magnified, thereby highlighting the need for adequate administrative, physical, and  
13 technical safeguards.<sup>14</sup>  
14  
15

16           60. Defendant knew and understood unprotected or exposed Private  
17 Information in the custody of insurance companies, like Defendant, is valuable and  
18 highly sought after by nefarious third parties seeking to illegally monetize that  
19 Private Information through unauthorized access.  
20  
21  
22  
23

---

24 <sup>12</sup> [https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=patientprotection](https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection)

25 <sup>13</sup> <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

26 <sup>14</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>  
27  
28

1           61. At all relevant times, Defendant knew, or reasonably should have  
2 known, of the importance of safeguarding the Private Information of Plaintiff and  
3 Class Members and of the foreseeable consequences that would occur if Defendant's  
4 data security system was breached, including, specifically, the significant costs that  
5 would be imposed on Plaintiff and Class Members as a result of a breach.  
6

7  
8           62. Plaintiff and Class Members now face years of constant surveillance of  
9 their financial and personal records, monitoring, and loss of rights. The Class is  
10 incurring and will continue to incur such damages in addition to any fraudulent use  
11 of their Private Information.  
12

13           63. The injuries to Plaintiff and Class Members were directly and  
14 proximately caused by Defendant's failure to implement or maintain adequate data  
15 security measures for the Private Information of Plaintiff and Class Members.  
16

17           64. The ramifications of Defendant's failure to keep secure the Private  
18 Information of Plaintiff and Class Members are long lasting and severe. Once Private  
19 Information is stolen—particularly Social Security numbers and PHI—fraudulent  
20 use of that information and damage to victims may continue for years.  
21

22           65. In the Notice Letter, Defendant makes an offer of 24 months of identity  
23 monitoring services. This is wholly inadequate to compensate Plaintiff and Class  
24 Members as it fails to provide for the fact victims of data breaches and other  
25 unauthorized disclosures commonly face multiple years of ongoing identity theft,  
26  
27  
28

1 financial fraud, and it entirely fails to provide sufficient compensation for the  
2 unauthorized release and disclosure of Plaintiff's and Class Members' Private  
3 Information.  
4

5 66. Defendant's offer of credit and identity monitoring establishes that  
6 Plaintiff's and Class Members' sensitive Private Information was in fact affected,  
7 accessed, compromised, and exfiltrated from Defendant's computer systems.  
8

9 67. As a healthcare entity in custody of the Private Information of its  
10 patients, Defendant knew, or should have known, the importance of safeguarding  
11 Private Information entrusted to it by Plaintiff and Class Members, and of the  
12 foreseeable consequences if its data security systems were breached. This includes  
13 the significant costs imposed on Plaintiff and Class Members as a result of a breach.  
14 Defendant failed, however, to take adequate cybersecurity measures to prevent the  
15 Data Breach.  
16  
17

### 18 *Value Of Private Information*

19

20 68. The Federal Trade Commission ("FTC") defines identity theft as "a  
21 fraud committed or attempted using the identifying information of another person  
22 without authority."<sup>15</sup> The FTC describes "identifying information" as "any name or  
23 number that may be used, alone or in conjunction with any other information, to  
24 identify a specific person," including, among other things, "[n]ame, Social Security  
25  
26

---

27 <sup>15</sup> 17 C.F.R. § 248.201 (2013).  
28

1 number, date of birth, official State or government issued driver's license or  
2 identification number, alien registration number, government passport number,  
3 employer or taxpayer identification number.”<sup>16</sup>  
4

5 69. The PII of individuals remains of high value to criminals, as evidenced  
6 by the prices they will pay through the dark web. Numerous sources cite dark web  
7 pricing for stolen identity credentials.<sup>17</sup>  
8

9 70. For example, Personal Information can be sold at a price ranging from  
10 \$40 to \$200.<sup>18</sup> Criminals can also purchase access to entire company data breaches  
11 from \$900 to \$4,500.<sup>19</sup>  
12

13 71. Moreover, Social Security numbers are among the worst kind of Private  
14 Information to have stolen because they may be put to a variety of fraudulent uses  
15 and are difficult for an individual to change.  
16

17 72. According to the Social Security Administration, each time an  
18 individual's Social Security number is compromised, “the potential for a thief to  
19 illegitimately gain access to bank accounts, credit cards, driving records, tax and  
20  
21  
22

---

23 <sup>16</sup> *Id.*

24 <sup>17</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.  
25 16, 2019, available at: [https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)  
26 [web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)

27 <sup>18</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,  
28 2017, available at: [https://www.experian.com/blogs/ask-experian/heres-how-much-your-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)  
personal-information-is-selling-for-on-the-dark-web/

<sup>19</sup> *In the Dark*, VPNOverview, 2019, available at: [https://vpnoverview.com/privacy/anonymous-](https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/)  
[browsing/in-the-dark/](https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/)

1 employment histories and other private information increases.”<sup>20</sup> Moreover,  
 2 “[b]ecause many organizations still use SSNs as the primary identifier, exposure to  
 3 identity theft and fraud remains.”<sup>21</sup>  
 4

5 73. The Social Security Administration stresses that the loss of an  
 6 individual’s Social Security number, as experienced by Plaintiff and some Class  
 7 Members, can lead to identity theft and extensive financial fraud:  
 8

9 A dishonest person who has your Social Security number can use it to  
 10 get other personal information about you. Identity thieves can use your  
 11 number and your good credit to apply for more credit in your name.  
 12 Then, they use the credit cards and don’t pay the bills, it damages your  
 13 credit. You may not find out that someone is using your number until  
 14 you’re turned down for credit, or you begin to get calls from unknown  
 15 creditors demanding payment for items you never bought. Someone  
 16 illegally using your Social Security number and assuming your identity  
 17 can cause a lot of problems.<sup>22</sup>  
 18

19 74. In fact, “[a] stolen Social Security number is one of the leading causes  
 20 of identity theft and can threaten your financial health.”<sup>23</sup> “Someone who has your  
 21 SSN can use it to impersonate you, obtain credit and open bank accounts, apply for  
 22

---

23 <sup>20</sup> See  
 24 <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

25 <sup>21</sup> *Id.*

26 <sup>22</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at:  
<https://www.ssa.gov/pubs/EN-05-10064.pdf>

27 <sup>23</sup> See <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/>  
 28

1 jobs, steal your tax refunds, get medical treatment, and steal your government  
2 benefits.”<sup>24</sup>

3  
4 75. What’s more, it is no easy task to change or cancel a stolen Social  
5 Security number. An individual cannot obtain a new Social Security number without  
6 significant paperwork and evidence of actual misuse. In other words, preventive  
7 action to defend against the possibility of misuse of a Social Security number is not  
8 permitted; an individual must show evidence of actual, ongoing fraud activity to  
9 obtain a new number.  
10

11  
12 76. Even then, a new Social Security number may not be effective.  
13 According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit  
14 bureaus and banks are able to link the new number very quickly to the old number,  
15 so all of that old bad information is quickly inherited into the new Social Security  
16 number.”<sup>25</sup>  
17

18  
19 77. For these reasons, some courts have referred to Social Security numbers  
20 as the “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-  
21 30111, 2019 WL 7946103, at \*12 (D. Mass. Dec. 31, 2019) (“Because Social  
22 Security numbers are the gold standard for identity theft, their theft is significant . .  
23  
24

25  
26 <sup>24</sup> See <https://www.investopedia.com/terms/s/ssn.asp>

27 <sup>25</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR  
28 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>



1 . . Access to Social Security numbers causes long-lasting jeopardy because the Social  
2 Security Administration does not normally replace Social Security numbers.”),  
3  
4 report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D.  
5 Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at  
6 \*4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs’ Social  
7 Security numbers are: arguably “the most dangerous type of personal information in  
8 the hands of identity thieves” because it is immutable and can be used to  
9 “impersonat[e] [the victim] to get medical services, government benefits, ... tax  
10 refunds, [and] employment.” . . . Unlike a credit card number, which can be changed  
11  
12 to eliminate the risk of harm following a data breach, “[a] social security number  
13 derives its value in that it is immutable,” and when it is stolen it can “forever be  
14 wielded to identify [the victim] and target her in fraudulent schemes and identity  
15 theft attacks.”)

16  
17  
18 78. Similarly, the California state government warns patients that:  
19  
20 “[o]riginally, your Social Security number (SSN) was a way for the government to  
21 track your earnings and pay you retirement benefits. But over the years, it has  
22 become much more than that. It is the key to a lot of your personal information. With  
23 your name and SSN, an identity thief could open new credit and bank accounts, rent  
24 an apartment, or even get a job.”<sup>26</sup>

25  
26  
27  
28  

---

<sup>26</sup> See <https://oag.ca.gov/idtheft/facts/your-ssn>

1           79. Driver's license numbers, which were compromised in the Data  
2 Breach, are incredibly valuable. "Hackers harvest license numbers because they're  
3 a very valuable piece of information."<sup>27</sup>  
4

5           80. A driver's license can be a critical part of a fraudulent, synthetic identity  
6 – which go for about \$1200 on the Dark Web. On its own, a forged license can sell  
7 for around \$200."<sup>28</sup>  
8

9           81. According to national credit bureau Experian:

10           A driver's license is an identity thief's paradise. With that one card, someone  
11 knows your birthdate, address, and even your height, eye color, and  
12 signature. If someone gets your driver's license number, it is also concerning  
13 because it's connected to your vehicle registration and insurance policies, as  
14 well as records on file with the Department of Motor Vehicles, place of  
15 employment (that keep a copy of your driver's license on file), doctor's  
16 office, government agencies, and other entities. Having access to that one  
17 number can provide an identity thief with several pieces of information they  
18 want to know about you. Next to your Social Security number, your driver's  
19 license number is one of the most important pieces of information to keep  
20 safe from thieves.  
21

22           82. According to cybersecurity specialty publication CPO Magazine, "[t]o  
23 those unfamiliar with the world of fraud, driver's license numbers might seem like  
24  
25  
26  
27  
28

---

24 <sup>27</sup> *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes,  
25 Apr. 20, 2021, available at: [https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658)  
26 [customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658) (last visited  
27 July 31, 2023).

28 <sup>28</sup> [https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658)  
[numbers-from-geico-in-months-long-breach/?sh=3e4755c38658](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658) (last visited on Feb. 21, 2023).

1 a relatively harmless piece of information to lose if it happens in isolation.”<sup>29</sup>

2 However, this is not the case. As cybersecurity experts point out:

3  
4 “It’s a gold mine for hackers. With a driver’s license number, bad actors can  
5 manufacture fake IDs, slotting in the number for any form that requires ID  
6 verification, or use the information to craft curated social engineering  
7 phishing attacks.”<sup>30</sup>

8 83. Victims of driver’s license number theft also often suffer  
9 unemployment benefit fraud, as described in a recent New York Times article.<sup>31</sup>

10 84. Theft of PHI is also gravely serious: “[a] thief may use your name or  
11 health insurance numbers to see a doctor, get prescription drugs, file claims with  
12 your insurance provider, or get other care. If the thief’s health information is mixed  
13 with yours, your treatment, insurance and payment records, and credit report may be  
14 affected.”<sup>32</sup>

15 85. The greater efficiency of electronic health records brings the risk of  
16 privacy breaches. These electronic health records contain a lot of sensitive  
17 information (e.g., patient data, patient diagnosis, lab results, medications,  
18 prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s  
19  
20  
21

22 <sup>29</sup> [https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-](https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/)  
23 [numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/](https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/) (last visited on  
24 Feb. 21, 2023).

25 <sup>30</sup> *Id.*

26 <sup>31</sup> *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at:  
27 <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last  
28 visited on Feb. 21, 2023).

29 <sup>32</sup> *Medical I.D. Theft*, EFraudPrevention  
30 [https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20yo,](https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20yo,ur,credit%20report%20may%20be%20affected.)  
31 [ur,credit%20report%20may%20be%20affected.](https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20yo,ur,credit%20report%20may%20be%20affected.) (last visited Nov. 6, 2023).

1 complete record can be sold for hundreds of dollars on the dark web. As such,  
2 PHI/PII is a valuable commodity for which a “cyber black market” exists where  
3 criminals openly post stolen payment card numbers, Social Security numbers, and  
4 other personal information on several underground internet websites.  
5 Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by  
6 cyberattacks, like the Data Breach here.  
7  
8

9 86. Between 2005 and 2019, at least 249 million people were affected by  
10 healthcare data breaches.<sup>33</sup> Indeed, during 2019 alone, over 41 million healthcare  
11 records were exposed, stolen, or unlawfully disclosed in 505 data breaches.<sup>34</sup> In  
12 short, these sorts of data breaches are increasingly common, especially among  
13 healthcare systems, which account for 30.03 percent of overall health data breaches,  
14 according to cybersecurity firm Tenable.<sup>35</sup>  
15  
16

17 87. According to account monitoring company LogDog, medical data sells  
18 for \$50 and up on the Dark Web.<sup>36</sup>  
19  
20  
21

---

22 <sup>33</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last  
23 accessed July 24, 2023).

24 <sup>34</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
25 July 24, 2023).

26 <sup>35</sup> [https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-  
27 incovid-19-era-breaches/](https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/) (last accessed July 24, 2023).

28 <sup>36</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security  
(Oct. 3, 2019), [https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-  
sometimes-crush-hospitals/#content](https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content) (last accessed July 20, 2021)

1           88. “Medical identity theft is a growing and dangerous crime that leaves its  
2 victims with little to no recourse for recovery,” reported Pam Dixon, executive  
3 director of World Privacy Forum. “Victims often experience financial repercussions  
4 and worse yet, they frequently discover erroneous information has been added to  
5 their personal medical files due to the thief’s activities.”<sup>37</sup>  
6

7  
8           89. A study by Experian found that the average cost of medical identity  
9 theft is “about \$20,000” per incident and that most victims of medical identity theft  
10 were forced to pay out-of-pocket costs for healthcare they did not receive to restore  
11 coverage.<sup>38</sup> Almost half of medical identity theft victims lose their healthcare  
12 coverage as a result of the incident, while nearly one-third of medical identity theft  
13 victims saw their insurance premiums rise, and 40 percent were never able to resolve  
14 their identity theft at all.<sup>39</sup>  
15  
16

17           90. Based on the foregoing, the information compromised in the Data  
18 Breach is significantly more valuable than the loss of, for example, credit card  
19 information in a retailer data breach because, there, victims can cancel or close credit  
20  
21  
22

---

23 <sup>37</sup> Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb.  
24 7, 2014, <https://khn.org/news/rise-of-indentity-theft/> (last accessed July 24, 2023).

25 <sup>38</sup> See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010),  
26 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed  
27 July 24, 2023).

28 <sup>39</sup> *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*,  
EXPERIAN, [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-  
toknow-about-them-and-what-to-do-after-one/](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/) (last accessed July 24, 2023).

1 and debit card accounts. The information compromised in this Data Breach is  
2 impossible to “close” and difficult, if not impossible, to change—Social Security  
3 numbers, PHI, dates of birth, and names.  
4

5 91. This data demands a much higher price on the black market. Martin  
6 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to  
7 credit card information, personally identifiable information and Social Security  
8 numbers are worth more than 10x on the black market.”<sup>40</sup>  
9

10 92. Among other forms of fraud, identity thieves may obtain driver’s  
11 licenses, government benefits, medical services, and housing or even give false  
12 information to police.  
13

14 93. The fraudulent activity resulting from the Data Breach may not come  
15 to light for years. There may be a time lag between when harm occurs versus when  
16 it is discovered, and also between when Private Information is stolen and when it is  
17 used. According to the U.S. Government Accountability Office (“GAO”), which  
18 conducted a study regarding data breaches:  
19  
20

21 [L]aw enforcement officials told us that in some cases, stolen data may  
22 be held for up to a year or more before being used to commit identity  
23 theft. Further, once stolen data have been sold or posted on the Web,  
24 fraudulent use of that information may continue for years. As a result,  
25

---

26 <sup>40</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
27 *Numbers*, IT World, (Feb. 6, 2015), available at:  
28 <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

1 studies that attempt to measure the harm resulting from data breaches  
2 cannot necessarily rule out all future harm.<sup>41</sup>

3 94. Plaintiff and Class Members now face years of constant surveillance of  
4 their financial and personal records, monitoring, and loss of rights. The Class is  
5 incurring and will continue to incur such damages in addition to any fraudulent use  
6 of their Private Information.  
7

8 ***Defendant Fails To Comply With FTC Guidelines***

9 95. The Federal Trade Commission (“FTC”) has promulgated numerous  
10 guides for businesses which highlight the importance of implementing reasonable  
11 data security practices. According to the FTC, the need for data security should be  
12 factored into all business decision-making.  
13

14 96. In 2016, the FTC updated its publication, Protecting Personal  
15 Information: A Guide for Business, which established cyber-security guidelines for  
16 businesses. These guidelines note that businesses should protect the personal patient  
17 information that they keep; properly dispose of personal information that is no longer  
18 needed; encrypt information stored on computer networks; understand their  
19 network’s vulnerabilities; and implement policies to correct any security problems.<sup>42</sup>  
20  
21  
22  
23  
24

25 <sup>41</sup> Report to Congressional Requesters, GAO, at 29 (June 2007), available at:  
26 <https://www.gao.gov/assets/gao-07-737.pdf>

27 <sup>42</sup> Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016).  
28 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

1        97. The guidelines also recommend that businesses use an intrusion  
2 detection system to expose a breach as soon as it occurs; monitor all incoming traffic  
3 for activity indicating someone is attempting to hack the system; watch for large  
4 amounts of data being transmitted from the system; and have a response plan ready  
5 in the event of a breach.<sup>43</sup>  
6

7  
8        98. The FTC further recommends that companies not maintain Private  
9 Information longer than is needed for authorization of a transaction; limit access to  
10 sensitive data; require complex passwords to be used on networks; use industry-  
11 tested methods for security; monitor for suspicious activity on the network; and  
12 verify that third-party service providers have implemented reasonable security  
13 measures.  
14

15  
16        99. The FTC has brought enforcement actions against businesses for failing  
17 to adequately and reasonably protect patient data, treating the failure to employ  
18 reasonable and appropriate measures to protect against unauthorized access to  
19 confidential patient data as an unfair act or practice prohibited by Section 5 of the  
20 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from  
21 these actions further clarify the measures businesses must take to meet their data  
22 security obligations.  
23  
24  
25  
26

---

27 <sup>43</sup> *Id.*  
28



1           100. These FTC enforcement actions include actions against healthcare  
2 providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2  
3 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at \*32 (MSNET July 28,  
4 2016) (“[T]he Commission concludes that LabMD’s data security practices were  
5 unreasonable and constitute an unfair act or practice in violation of Section 5 of the  
6 FTC Act.”).

7  
8  
9           101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices  
10 in or affecting commerce,” including, as interpreted and enforced by the FTC, the  
11 unfair act or practice by businesses, such as Defendant, of failing to use reasonable  
12 measures to protect Private Information. The FTC publications and orders described  
13 above also form part of the basis of Defendant's duty in this regard.  
14  
15

16           102. Defendant failed to properly implement basic data security practices.

17           103. Defendant's failure to employ reasonable and appropriate measures to  
18 protect against unauthorized access to the Private Information of its patients or to  
19 comply with applicable industry standards constitutes an unfair act or practice  
20 prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.  
21

22           104. Upon information and belief, Hope was at all times fully aware of its  
23 obligation to protect the Private Information of its patients, Hope was also aware of  
24 the significant repercussions that would result from its failure to do so. Accordingly,  
25 Defendant's conduct was particularly unreasonable given the nature and amount of  
26  
27  
28

1 Private Information it obtained and stored and the foreseeable consequences of the  
2 immense damages that would result to Plaintiff and the Class.

3  
4 ***Defendant Fails To Comply With HIPAA Guidelines***

5 105. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and  
6 is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.  
7 Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually  
8 Identifiable Health Information”), and Security Rule (“Security Standards for the  
9 Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part  
10 164, Subparts A and C.

11  
12  
13 106. Defendant is subject to the rules and regulations for safeguarding  
14 electronic forms of medical information pursuant to the Health Information  
15 Technology Act (“HITECH”).<sup>44</sup> See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

16  
17 107. HIPAA’s Privacy Rule or *Standards for Privacy of Individually*  
18 *Identifiable Health Information* establishes national standards for the protection of  
19 health information.

20  
21 108. HIPAA’s Privacy Rule or *Security Standards for the Protection of*  
22 *Electronic Protected Health Information* establishes a national set of security  
23

24  
25  
26  
27 <sup>44</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining  
28 protected health information. HITECH references and incorporates HIPAA.

1 standards for protecting health information that is kept or transferred in electronic  
2 form.

3  
4 109. HIPAA requires “compl[iance] with the applicable standards,  
5 implementation specifications, and requirements” of HIPAA “with respect to  
6 electronic protected health information.” 45 C.F.R. § 164.302.

7  
8 110. “Electronic protected health information” is “individually identifiable  
9 health information ... that is (i) transmitted by electronic media; maintained in  
10 electronic media.” 45 C.F.R. § 160.103.

11  
12 111. HIPAA’s Security Rule requires Defendant to do the following:

- 13 a. Ensure the confidentiality, integrity, and availability of all  
14 electronic protected health information the covered entity or  
15 business associate creates, receives, maintains, or transmits;  
16  
17 b. Protect against any reasonably anticipated threats or hazards to  
18 the security or integrity of such information;  
19  
20 c. Protect against any reasonably anticipated uses or disclosures of  
21 such information that are not permitted; and  
22  
23 d. Ensure compliance by its workforce.

24 112. HIPAA also requires Defendant to “review and modify the security  
25 measures implemented ... as needed to continue provision of reasonable and  
26 appropriate protection of electronic protected health information.” 45 C.F.R. §  
27  
28

1 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement  
2 technical policies and procedures for electronic information systems that maintain  
3 electronic protected health information to allow access only to those persons or  
4 software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).  
5

6 113. HIPAA and HITECH also obligated Defendant to implement policies  
7 and procedures to prevent, detect, contain, and correct security violations, and to  
8 protect against uses or disclosures of electronic protected health information that are  
9 reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. §  
10 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.  
11  
12

13 114. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also  
14 requires Defendant to provide notice of the Data Breach to each affected individual  
15 “without unreasonable delay and *in no case later than 60 days following discovery*  
16 *of the breach.*”<sup>45</sup>  
17

18 115. HIPAA requires a covered entity to have and apply appropriate  
19 sanctions against members of its workforce who fail to comply with the privacy  
20 policies and procedures of the covered entity or the requirements of 45 C.F.R. Part  
21 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).  
22  
23  
24  
25  
26

---

27 <sup>45</sup> Breach Notification Rule, U.S. Dep’t of Health & Human Services,  
28 <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

1           116. HIPAA requires a covered entity to mitigate, to the extent practicable,  
2 any harmful effect that is known to the covered entity of a use or disclosure of  
3 protected health information in violation of its policies and procedures or the  
4 requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business  
5 associate. *See* 45 C.F.R. § 164.530(f).  
6

7  
8           117. HIPAA also requires the Office of Civil Rights (“OCR”), within the  
9 Department of Health and Human Services (“HHS”), to issue annual guidance  
10 documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-  
11 164.318. For example, “HHS has developed guidance and tools to assist HIPAA  
12 covered entities in identifying and implementing the most cost effective and  
13 appropriate administrative, physical, and technical safeguards to protect the  
14 confidentiality, integrity, and availability of e-PHI and comply with the risk analysis  
15 requirements of the Security Rule.” US Department of Health & Human Services,  
16 Security Rule Guidance Material.<sup>46</sup> The list of resources includes a link to guidelines  
17 set by the National Institute of Standards and Technology (NIST), which OCR says  
18 “represent the industry standard for good business practices with respect to standards  
19 for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk  
20 Analysis.<sup>47</sup>  
21  
22  
23  
24

25  
26 <sup>46</sup> <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

27 <sup>47</sup> [https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-  
28 analysis/index.html](https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html)

***Defendant Fails To Comply With Industry Standards***

118. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

119. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Hope failed to follow these industry best practices, including a failure to implement multi-factor authentication.

120. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Hope failed to follow these cybersecurity best practices, including failure to train staff.

121. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

122. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

### ***Common Injuries & Damages***

123. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the

1 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual  
2 consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages;  
3 and (ix) the continued and certainly increased risk to their Private Information,  
4 which: (a) remains unencrypted and available for unauthorized third parties to access  
5 and abuse; and (b) remains backed up in Defendant's possession and is subject to  
6 further unauthorized disclosures so long as Defendant fails to undertake appropriate  
7 and adequate measures to protect the Private Information.  
8

9  
10 ***Data Breaches Increase Victims' Risk Of Identity Theft***

11  
12 124. As Plaintiff has already experienced, the unencrypted Private  
13 Information of Class Members will end up for sale on the dark web as that is the  
14 *modus operandi* of hackers.  
15

16 125. Unencrypted Private Information may also fall into the hands of  
17 companies that will use the detailed Private Information for targeted marketing  
18 without the approval of Plaintiff and Class Members. Simply put, unauthorized  
19 individuals can easily access the Private Information of Plaintiff and Class Members.  
20

21 126. The link between a data breach and the risk of identity theft is simple  
22 and well established. Criminals acquire and steal Private Information to monetize  
23 the information. Criminals monetize the data by selling the stolen information on the  
24 black market to other criminals who then utilize the information to commit a variety  
25 of identity theft related crimes discussed below.  
26  
27  
28



1           127. Plaintiff's and Class Members' Private Information is of great value to  
2 hackers and cyber criminals, and the data stolen in the Data Breach has been used  
3 and will continue to be used in a variety of sordid ways for criminals to exploit  
4 Plaintiff and Class Members and to profit off their misfortune.  
5

6           128. Due to the risk of one's Social Security number being exposed, state  
7 legislatures have passed laws in recognition of the risk: "[t]he social security number  
8 can be used as a tool to perpetuate fraud against a person and to acquire sensitive  
9 personal, financial, medical, and familial information, the release of which could  
10 cause great financial or personal harm to an individual. While the social security  
11 number was intended to be used solely for the administration of the federal Social  
12 Security System, over time this unique numeric identifier has been used extensively  
13 for identity verification purposes[.]"<sup>48</sup>  
14  
15  
16

17           129. Moreover, "SSNs have been central to the American identity  
18 infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes  
19 have also had SSNs baked into their identification process for years. In fact, SSNs  
20 have been the gold standard for identifying and verifying the credit history of  
21 prospective patients."<sup>49</sup>  
22  
23  
24  
25

---

26 <sup>48</sup> See N.C. Gen. Stat. § 132-1.10(1).

27 <sup>49</sup> See [https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-](https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers)  
28 [numbers](https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers)

130. “Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation’s largest 25 banks have stopped using the numbers to verify a patient’s identity after the initial account setup[.]”<sup>50</sup> Accordingly, since Social Security numbers are frequently used to verify an individual’s identity after logging onto an account or attempting a transaction, “[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account”<sup>51</sup>

131. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.<sup>52</sup>

---

<sup>50</sup> See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>

<sup>51</sup> See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

<sup>52</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>)

1           132. With “Fullz” packages, cyber-criminals can cross-reference two  
2 sources of Private Information to marry unregulated data available elsewhere to  
3 criminally stolen data with an astonishingly complete scope and degree of accuracy  
4 in order to assemble complete dossiers on individuals.  
5

6           133. The development of “Fullz” packages means here that the stolen Private  
7 Information from the Data Breach can easily be used to link and identify it to  
8 Plaintiff’s and Class Members’ phone numbers, email addresses, and other  
9 unregulated sources and identifiers. In other words, even if certain information such  
10 as emails, phone numbers, or credit card numbers may not be included in the Private  
11 Information that was exfiltrated in the Data Breach, criminals may still easily create  
12 a Fullz package and sell it at a higher price to unscrupulous operators and criminals  
13 (such as illegal and scam telemarketers) over and over.  
14  
15  
16

17           134. The existence and prevalence of “Fullz” packages means that the  
18 Private Information stolen from the data breach can easily be linked to the  
19 unregulated data (like insurance information) of Plaintiff and the other Class  
20 Members.  
21

22           135. Thus, even if certain information (such as insurance information) was  
23 not stolen in the data breach, criminals can still easily create a comprehensive  
24 “Fullz” package.  
25  
26  
27  
28

1           136. Then, this comprehensive dossier can be sold—and then resold in  
2 perpetuity—to crooked operators and other criminals (like illegal and scam  
3 telemarketers).  
4

5           ***Loss Of Time To Mitigate Risk Of Identity Theft & Fraud***

6           137. As a result of the recognized risk of identity theft, when a Data Breach  
7 occurs, and an individual is notified by a company that their Private Information was  
8 compromised, as in this Data Breach, the reasonable person is expected to take steps  
9 and spend time to address the dangerous situation, learn about the breach, and  
10 otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to  
11 spend time taking steps to review accounts or credit reports could expose the  
12 individual to greater financial harm – yet, the resource and asset of time has been  
13 lost.  
14  
15  
16

17           138. Thus, due to the actual and imminent risk of identity theft, Defendant,  
18 in its Notice Letter instructs Plaintiff and Class Members to take the following  
19 measures to protect themselves: “[w]e encourage you to remain vigilant to protect  
20 against potential fraud and identity theft by reviewing your account statements,  
21 monitoring your credit reports, and notifying your financial institutions of any  
22 potential suspicious activity.”<sup>53</sup>  
23  
24  
25  
26

---

27           <sup>53</sup> Notice Letter.  
28

1           139. In addition, Defendant's Notice letter includes a full two pages devoted  
2 to "Steps You Can Take To Help Protect Your Information" that recommend  
3 Plaintiff and Class Members to partake in activities such as enrolling in the credit  
4 monitoring services offered by Defendant, obtaining credit reports, and contacting  
5 government agencies.<sup>54</sup>  
6

7  
8           140. Defendant's extensive suggestion of steps that Plaintiff and Class  
9 Members must take in order to protect themselves from identity theft and/or fraud  
10 demonstrates the significant time that Plaintiffs and Class Members must undertake  
11 in response to the Data Breach. Plaintiff's and Class Members' time is highly  
12 valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered  
13 actual injury and damages in the form of lost time that they spent on mitigation  
14 activities in response to the Data Breach and at the direction of Defendant's Notice  
15 Letter.  
16  
17

18           141. Plaintiff and Class Members have spent, and will spend additional time  
19 in the future, on a variety of prudent actions, such as researching and verifying the  
20 legitimacy of the Data Breach, signing up for credit monitoring and identity theft  
21 protection services, and monitoring their financial accounts for any indication of  
22 fraudulent activity, which may take years to detect. Accordingly, the Data Breach  
23  
24  
25  
26

---

27 <sup>54</sup> *Id.*  
28

1 has caused Plaintiff and Class Members to suffer actual injury in the form of lost  
2 time—which cannot be recaptured—spent on mitigation activities.

3  
4 142. Plaintiff’s mitigation efforts are consistent with the U.S. Government  
5 Accountability Office that released a report in 2007 regarding data breaches (“GAO  
6 Report”) in which it noted that victims of identity theft will face “substantial costs  
7 and time to repair the damage to their good name and credit record.”<sup>55</sup>  
8

9 143. Plaintiff’s mitigation efforts are also consistent with the steps that FTC  
10 recommends that data breach victims take several steps to protect their personal and  
11 financial information after a data breach, including: contacting one of the credit  
12 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven  
13 years if someone steals their identity), reviewing their credit reports, contacting  
14 companies to remove fraudulent charges from their accounts, placing a credit freeze  
15 on their credit, and correcting their credit reports.<sup>56</sup>  
16  
17

18 144. And for those Class Members who experience actual identity theft and  
19 fraud, the United States Government Accountability Office released a report in 2007  
20 regarding data breaches (“GAO Report”) in which it noted that victims of identity  
21 theft will face “substantial costs and time to repair the damage to their good name  
22 and credit record.”<sup>[4]</sup>  
23  
24

25  
26 <sup>55</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data  
27 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full  
Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

28 <sup>56</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

### ***Diminution of Value of Private Information***

145. PII and PHI are valuable property rights.<sup>57</sup> Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

146. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>58</sup>

147. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>59</sup>

148. In fact, the data marketplace is so sophisticated that patients can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>60,61</sup>

<sup>57</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

<sup>58</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

<sup>59</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

<sup>60</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>61</sup> <https://datacoup.com/>

1 149. Consumers who agree to provide their web browsing history to the  
 2 Nielsen Corporation can receive up to \$50.00 a year.<sup>62</sup>

3  
 4 150. Theft of PHI is also gravely serious: “[a] thief may use your name or  
 5 health insurance numbers to see a doctor, get prescription drugs, file claims with  
 6 your insurance provider, or get other care. If the thief’s health information is mixed  
 7 with yours, your treatment, insurance and payment records, and credit report may be  
 8 affected.”<sup>63</sup>

9  
 10 151. As a result of the Data Breach, Plaintiff’s and Class Members’ Private  
 11 Information, which has an inherent market value in both legitimate and dark markets,  
 12 has been damaged and diminished by its compromise and unauthorized release.  
 13 However, this transfer of value occurred without any consideration paid to Plaintiff  
 14 or Class Members for their property, resulting in an economic loss. Moreover, the  
 15 Private Information is now readily available, and the rarity of the Data has been lost,  
 16 thereby causing additional loss of value.  
 17  
 18  
 19

20 152. At all relevant times, Hope knew, or reasonably should have known, of  
 21 the importance of safeguarding the Private Information of Plaintiff and Class  
 22 Members, and of the foreseeable consequences that would occur if Defendant's data  
 23

24  
 25 <sup>62</sup> <https://digi.me/what-is-digime/>

26 <sup>63</sup> *Medical I.D. Theft*, EFraudPrevention  
 27 <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).  
 28



1 security system was breached, including, specifically, the significant costs that  
2 would be imposed on Plaintiff and Class Members as a result of a breach.

3  
4 153. The fraudulent activity resulting from the Data Breach may not come  
5 to light for years.

6 154. Plaintiff and Class Members now face years of constant surveillance of  
7 their financial and personal records, monitoring, and loss of rights. The Class is  
8 incurring and will continue to incur such damages in addition to any fraudulent use  
9 of their Private Information.  
10

11  
12 155. Hope was, or should have been, fully aware of the unique type and the  
13 significant volume of data on Defendant's network, amounting to more than eight  
14 hundred thousand individuals' detailed personal information and, thus, the  
15 significant number of individuals who would be harmed by the exposure of the  
16 unencrypted data.  
17

18 156. The injuries to Plaintiff and Class Members were directly and  
19 proximately caused by Defendant's failure to implement or maintain adequate data  
20 security measures for the Private Information of Plaintiff and Class Members.  
21

22 ***Future Cost of Credit and Identity Theft Monitoring is Reasonable and***  
23 ***Necessary***

24 157. Given the type of targeted attack in this case, sophisticated criminal  
25 activity, the type of Private Information involved, and Plaintiff's Private Information  
26 already being disseminated on the dark web (as discussed below), there is a strong  
27  
28

1 probability that entire batches of stolen information have been placed, or will be  
2 placed, on the black market/dark web for sale and purchase by criminals intending  
3 to utilize the Private Information for identity theft crimes –e.g., opening bank  
4 accounts in the victims’ names to make purchases or to launder money; file false tax  
5 returns; take out loans or lines of credit; or file false unemployment claims.  
6

7  
8 158. Such fraud may go undetected until debt collection calls commence  
9 months, or even years, later. An individual may not know that his or her Private  
10 Information was used to file for unemployment benefits until law enforcement  
11 notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are  
12 typically discovered only when an individual’s authentic tax return is rejected.  
13

14 159. Consequently, Plaintiff and Class Members are at an increased risk of  
15 fraud and identity theft for many years into the future.  
16

17 160. The retail cost of credit monitoring and identity theft monitoring can  
18 cost around \$200 a year per Class Member. This is reasonable and necessary cost to  
19 monitor to protect Class Members from the risk of identity theft that arose from  
20 Defendant’s Data Breach.  
21

22 ***Loss Of Benefit Of The Bargain***  
23

24 161. Furthermore, Defendant’s poor data security practices deprived  
25 Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay  
26 Defendant and/or its agents for the provision of healthcare services, Plaintiff and  
27  
28

1 other reasonable patients understood and expected that they were, in part, paying for  
2 the healthcare services and necessary data security to protect the Private Information,  
3 when in fact, Defendant did not provide the expected data security. Accordingly,  
4 Plaintiff and Class Members received healthcare services that were of a lesser value  
5 than what they reasonably expected to receive under the bargains they struck with  
6 Defendant.  
7

8  
9 ***Plaintiff Lynsey Saurenmann's Experience***

10 162. Plaintiff Lynsey Saurenmann is a current Hope patient.

11  
12 163. As a condition of obtaining healthcare services at Hope, she was  
13 required to provide her Private Information to Defendant, including her name, date  
14 of birth, contact information, health insurance information, Social Security number,  
15 and other sensitive information.  
16

17 164. At the time of the Data Breach—September 19, 2023 through Octboer  
18 12, 2023--Defendant maintained Plaintiff's Private Information in its system.  
19

20 165. Plaintiff Saurenmann is very careful about sharing her sensitive Private  
21 Information. Plaintiff stores any documents containing her Private Information in a  
22 safe and secure location. She has never knowingly transmitted unencrypted sensitive  
23 Private Information over the internet or any other unsecured source. Plaintiff would  
24 not have entrusted her Private Information to Defendant had she known of  
25 Defendant's lax data security policies.  
26  
27  
28

1           166. Plaintiff Lynsey Saurenmann received the Notice Letter, by U.S. mail,  
2 directly from Defendant, dated April 2, 2024. According to the Notice Letter,  
3 Plaintiff's Private Information was improperly accessed and obtained by  
4 unauthorized third parties, including her name, contact information (e.g., email  
5 address, phone number), date of birth, social security number, driver's license or  
6 other government identification, financial details (e.g., bank account number and/or  
7 credit card details), health insurance information, medical records and information  
8 about medical history and/or associated conditions, and/ or unique identifiers to  
9 associate individuals with City of Hope (e.g., medical record number).

13           167. As a result of the Data Breach, and at the direction of Defendant's  
14 Notice Letter, which instructs Plaintiff to "remain vigilant to protect against potential  
15 fraud and identity theft by reviewing your account statements, monitoring your  
16 credit reports, and notifying your financial institutions of any potential suspicious  
17 activity[,]”<sup>64</sup> Plaintiff made reasonable efforts to mitigate the impact of the Data  
18 Breach, including researching and verifying the legitimacy of the Data Breach,  
19 signing up for credit monitoring and identity theft protection services, and  
20 monitoring her financial accounts for any indication of fraudulent activity, which  
21 may take years to detect. Plaintiff has spent significant time dealing with the Data  
22 Breach—valuable time Plaintiff otherwise would have spent on other activities,  
23  
24  
25  
26

---

27 <sup>64</sup> Notice Letter.  
28

1 including but not limited to work and/or recreation. This time has been lost forever  
2 and cannot be recaptured.

3  
4 168. Plaintiff suffered actual injury from having her Private Information  
5 compromised as a result of the Data Breach including, but not limited to: (i) invasion  
6 of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of  
7 Private Information; (iv) lost time and opportunity costs associated with attempting  
8 to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the  
9 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual  
10 consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages;  
11 and (ix) the continued and certainly increased risk to her Private Information, which:  
12 (a) remains unencrypted and available for unauthorized third parties to access and  
13 abuse; and (b) remains backed up in Defendant's possession and is subject to further  
14 unauthorized disclosures so long as Defendant fails to undertake appropriate and  
15 adequate measures to protect the Private Information.  
16  
17  
18  
19

20 169. Plaintiff additionally suffered actual injury in the form of her Private  
21 Information being disseminated on the dark web, according to Experian and Credit  
22 Karma, which, upon information and belief, was caused by the Data Breach.  
23

24 170. Plaintiff additionally suffered actual injury in the form of experiencing  
25 an increase in spam calls, texts, and/or emails, which, upon information and belief,  
26 was caused by the Data Breach. This misuse of her PII was caused, upon information  
27  
28

1 and belief, by the fact that cybercriminals are able to easily use the information  
2 compromised in the Data Breach to find more information about an individual, such  
3 as their phone number or email address, from publicly available sources, including  
4 websites that aggregate and associate personal information with the owner of such  
5 information.  
6

7  
8 171. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress,  
9 which has been compounded by the fact that Defendant has still not fully informed  
10 her of key details about the Data Breach's occurrence.  
11

12 172. As a result of the Data Breach, Plaintiff anticipates spending  
13 considerable time and money on an ongoing basis to try to mitigate and address  
14 harms caused by the Data Breach.  
15

16 173. As a result of the Data Breach, Plaintiff is at a present risk and will  
17 continue to be at increased risk of identity theft and fraud for years to come.  
18

19 174. Plaintiff Lynsey Saurenmann has a continuing interest in ensuring that  
20 her Private Information, which, upon information and belief, remains backed up in  
21 Defendant's possession, is protected and safeguarded from future breaches.  
22

### 23 **CLASS ALLEGATIONS**

24 175. Plaintiff brings this nationwide class action on behalf of herself and on  
25 behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and  
26 23(c)(4) of the Federal Rules of Civil Procedure.  
27  
28

176. The Classes that Plaintiff seeks to represent is defined as follows:

**Nationwide Class**

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the “Class”).

**California Subclass**

All individuals residing in the state of California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the “California Subclass”).

177. Excluded from the Classes are the following individuals and/or entities:

Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

178. Plaintiff reserves the right to amend the definitions of the Class and/or California Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

179. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 827,000 Class

1 Members were impacted in the Data Breach.<sup>65</sup> The Class is apparently identifiable  
2 within Defendant's records, and Defendant has already identified these individuals  
3 (as evidenced by sending them breach notification letters).  
4

5 180. Common questions of law and fact exist as to all members of the Class  
6 and predominate over any questions affecting solely individual members of the  
7 Class. Among the questions of law and fact common to the Class that predominate  
8 over questions which may affect individual Class members, including the following:  
9

- 10 a. Whether and to what extent Defendant had a duty to protect the Private  
11 Information of Plaintiff and Class Members;  
12
- 13 b. Whether Defendant had respective duties not to disclose the Private  
14 Information of Plaintiff and Class Members to unauthorized third  
15 parties;  
16
- 17 c. Whether Defendant had respective duties not to use the Private  
18 Information of Plaintiff and Class Members for non-business purposes;  
19
- 20 d. Whether Defendant failed to adequately safeguard the Private  
21 Information of Plaintiff and Class Members;  
22
- 23 e. Whether and when Defendant actually learned of the Data Breach;  
24  
25  
26

---

27 <sup>65</sup> See <https://apps.web.maine.gov/online/aewviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml>  
28



- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

181. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to

1 virtually identical conduct and now suffers from the same violations of the law as  
2 each other member of the Class.

3  
4 182. Policies Generally Applicable to the Class: This class action is also  
5 appropriate for certification because Defendant acted or refused to act on grounds  
6 generally applicable to the Class, thereby requiring the Court's imposition of  
7 uniform relief to ensure compatible standards of conduct toward the Class Members  
8 and making final injunctive relief appropriate with respect to the Class as a whole.  
9 Defendant's policies challenged herein apply to and affect Class Members uniformly  
10 and Plaintiff's challenges of these policies hinges on Defendant's conduct with  
11 respect to the Class as a whole, not on facts or law applicable only to Plaintiff.  
12  
13

14 183. Adequacy: Plaintiff will fairly and adequately represent and protect the  
15 interests of the Class Members in that she has no disabling conflicts of interest that  
16 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief  
17 that is antagonistic or adverse to the Class Members and the infringement of the  
18 rights and the damages she has suffered are typical of other Class Members. Plaintiff  
19 has retained counsel experienced in complex class action and data breach litigation,  
20 and Plaintiff intend to prosecute this action vigorously.  
21  
22  
23

24 184. Superiority and Manageability: The class litigation is an appropriate  
25 method for fair and efficient adjudication of the claims involved. Class action  
26 treatment is superior to all other available methods for the fair and efficient  
27  
28

1 adjudication of the controversy alleged herein; it will permit a large number of Class  
2 Members to prosecute their common claims in a single forum simultaneously,  
3 efficiently, and without the unnecessary duplication of evidence, effort, and expense  
4 that hundreds of individual actions would require. Class action treatment will permit  
5 the adjudication of relatively modest claims by certain Class Members, who could  
6 not individually afford to litigate a complex claim against large corporations, like  
7 Defendant. Further, even for those Class Members who could afford to litigate such  
8 a claim, it would still be economically impractical and impose a burden on the courts.  
9

10  
11  
12 185. The nature of this action and the nature of laws available to Plaintiff  
13 and Class Members make the use of the class action device a particularly efficient  
14 and appropriate procedure to afford relief to Plaintiff and Class Members for the  
15 wrongs alleged because Defendant would necessarily gain an unconscionable  
16 advantage since they would be able to exploit and overwhelm the limited resources  
17 of each individual Class Member with superior financial and legal resources; the  
18 costs of individual suits could unreasonably consume the amounts that would be  
19 recovered; proof of a common course of conduct to which Plaintiff was exposed is  
20 representative of that experienced by the Class and will establish the right of each  
21 Class Member to recover on the cause of action alleged; and individual actions  
22 would create a risk of inconsistent results and would be unnecessary and duplicative  
23 of this litigation.  
24  
25  
26  
27  
28

1           186. The litigation of the claims brought herein is manageable. Defendant's  
2 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable  
3 identities of Class Members demonstrates that there would be no significant  
4 manageability problems with prosecuting this lawsuit as a class action.  
5

6           187. Adequate notice can be given to Class Members directly using  
7 information maintained in Defendant's records.  
8

9           188. Unless a Class-wide injunction is issued, Defendant may continue in its  
10 failure to properly secure the Private Information of Class Members, Defendant may  
11 continue to refuse to provide proper notification to Class Members regarding the  
12 Data Breach, and Defendant may continue to act unlawfully as set forth in this  
13 Complaint.  
14

15           189. Further, Defendant has acted on grounds that apply generally to the  
16 Class as a whole, so that class certification, injunctive relief, and corresponding  
17 declaratory relief are appropriate on a class- wide basis.  
18

19           190. Likewise, particular issues under Rule 42(d)(1) are appropriate for  
20 certification because such claims present only particular, common issues, the  
21 resolution of which would advance the disposition of this matter and the parties'  
22 interests therein. Such particular issues include, but are not limited to:  
23

- 24           a. Whether Defendant failed to timely notify the Plaintiff and the class of  
25 the Data Breach;  
26  
27  
28

- 1 b. Whether Defendant owed a legal duty to Plaintiff and the Class to  
2 exercise due care in collecting, storing, and safeguarding their Private  
3 Information;  
4  
5 c. Whether Defendant's security measures to protect their data systems  
6 were reasonable in light of best practices recommended by data security  
7 experts;  
8  
9 d. Whether Defendant's failure to institute adequate protective security  
10 measures amounted to negligence;  
11  
12 e. Whether Defendant failed to take commercially reasonable steps to  
13 safeguard patient Private Information; and Whether adherence to FTC  
14 data security recommendations, and measures recommended by data  
15 security experts would have reasonably prevented the Data Breach.  
16

17 **CAUSES OF ACTION**

18 **COUNT I**

19 **Negligence**

20 **(On Behalf of Plaintiff and the Class)**

21 191. Plaintiff re-alleges and incorporates by reference all preceding  
22 allegations, as if fully set forth herein.  
23

24 192. Defendant requires its patients, including Plaintiff and Class Members,  
25 to submit non-public Private Information in the ordinary course of providing its  
26 healthcare services.  
27  
28

1           193. Defendant gathered and stored the Private Information of Plaintiff and  
2 Class Members as part of its business of soliciting its services to its patients, which  
3 solicitations and services affect commerce.  
4

5           194. Plaintiff and Class Members entrusted Defendant with their Private  
6 Information with the understanding that Defendant would safeguard their  
7 information.  
8

9           195. Defendant had full knowledge of the sensitivity of the Private  
10 Information and the types of harm that Plaintiff and Class Members could and would  
11 suffer if the Private Information were wrongfully disclosed.  
12

13           196. By voluntarily undertaking and assuming the responsibility to collect  
14 and store this data, and in fact doing so, and sharing it and using it for commercial  
15 gain, Defendant had a duty of care to use reasonable means to secure and safeguard  
16 their computer property—and Class Members' Private Information held within it—  
17 to prevent disclosure of the information, and to safeguard the information from theft.  
18 Defendant's duty included a responsibility to implement processes by which they  
19 could detect a breach of its security systems in a reasonably expeditious period of  
20 time and to give prompt notice to those affected in the case of a data breach.  
21  
22  
23

24           197. Defendant had a duty to employ reasonable security measures under  
25 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits  
26 “unfair . . . practices in or affecting commerce,” including, as interpreted and  
27  
28

1 enforced by the FTC, the unfair practice of failing to use reasonable measures to  
2 protect confidential data.

3  
4 198. Defendant's duty to use reasonable security measures under HIPAA  
5 required Defendant to "reasonably protect" confidential data from "any intentional  
6 or unintentional use or disclosure" and to "have in place appropriate administrative,  
7 technical, and physical safeguards to protect the privacy of protected health  
8 information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical  
9 information at issue in this case constitutes "protected health information" within the  
10 meaning of HIPAA.  
11  
12

13 199. For instance, HIPAA required Defendant to notify victims of the  
14 Breach within 60 days of the discovery of the Data Breach. Defendant did not begin  
15 to notify Plaintiff or Class Members of the Data Breach until April 2, 2024 despite,  
16 upon information and belief, Defendant knowing shortly after October 13, 2023 that  
17 unauthorized persons had accessed and acquired the private, protected, personal  
18 information of Plaintiff and the Class.  
19  
20

21 200. Defendant owed a duty of care to Plaintiff and Class Members to  
22 provide data security consistent with industry standards and other requirements  
23 discussed herein, and to ensure that its systems and networks adequately protected  
24 the Private Information.  
25  
26  
27  
28

1           201. Defendant's duty of care to use reasonable security measures arose as a  
2 result of the special relationship that existed between Hope and Plaintiff and Class  
3 Members. That special relationship arose because Plaintiff and the Class entrusted  
4 Hope with their confidential Private Information, a necessary part of being patients  
5 at Defendant.  
6

7  
8           202. Defendant's duty to use reasonable care in protecting confidential data  
9 arose not only as a result of the statutes and regulations described above, but also  
10 because Defendant is bound by industry standards to protect confidential Private  
11 Information.  
12

13           203. Defendant was subject to an "independent duty," untethered to any  
14 contract between Defendant and Plaintiff or the Class.  
15

16           204. Defendant also had a duty to exercise appropriate clearinghouse  
17 practices to remove former patients' Private Information it was no longer required  
18 to retain pursuant to regulations.  
19

20           205. Moreover, Defendant had a duty to promptly and adequately notify  
21 Plaintiff and the Class of the Data Breach.  
22

23           206. Defendant had and continues to have a duty to adequately disclose that  
24 the Private Information of Plaintiff and the Class within Defendant's possession  
25 might have been compromised, how it was compromised, and precisely the types of  
26 data that were compromised and when. Such notice was necessary to allow Plaintiff  
27  
28



1 and the Class to take steps to prevent, mitigate, and repair any identity theft and the  
2 fraudulent use of their Private Information by third parties.

3  
4 207. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and  
5 other applicable standards, and thus was negligent, by failing to use reasonable  
6 measures to protect Class Members' Private Information. The specific negligent acts  
7 and omissions committed by Defendant include, but are not limited to, the following:  
8

- 9 a. Failing to adopt, implement, and maintain adequate security measures  
10 to safeguard Class Members' Private Information;  
11  
12 b. Failing to adequately monitor the security of their networks and  
13 systems;  
14  
15 c. Allowing unauthorized access to Class Members' Private Information;  
16  
17 d. Failing to detect in a timely manner that Class Members' Private  
18 Information had been compromised;  
19  
20 e. Failing to remove former patients' Private Information it was no longer  
21 required to retain pursuant to regulations, and  
22  
23 f. Failing to timely and adequately notify Class Members about the Data  
24 Breach's occurrence and scope, so that they could take appropriate  
25 steps to mitigate the potential for identity theft and other damages.

26 208. Defendant violated Section 5 of the FTC Act and HIPAA by failing to  
27 use reasonable measures to protect Private Information and not complying with  
28

1 applicable industry standards, as described in detail herein. Defendant's conduct was  
2 particularly unreasonable given the nature and amount of Private Information it  
3 obtained and stored and the foreseeable consequences of the immense damages that  
4 would result to Plaintiff and the Class.  
5

6         209. Plaintiff and Class Members were within the class of persons the  
7 Federal Trade Commission Act and HIPAA were intended to protect and the type of  
8 harm that resulted from the Data Breach was the type of harm that the statutes were  
9 intended to guard against.  
10

11         210. Defendant's violation of Section 5 of the FTC Act and HIPAA  
12 constitutes negligence.  
13

14         211. The FTC has pursued enforcement actions against businesses, which,  
15 as a result of their failure to employ reasonable data security measures and avoid  
16 unfair and deceptive practices, caused the same harm as that suffered by Plaintiff  
17 and the Class.  
18

19         212. A breach of security, unauthorized access, and resulting injury to  
20 Plaintiff and the Class was reasonably foreseeable, particularly in light of  
21 Defendant's inadequate security practices.  
22

23         213. It was foreseeable that Defendant's failure to use reasonable measures  
24 to protect Class Members' Private Information would result in injury to Class  
25  
26  
27  
28

1 Members. Further, the breach of security was reasonably foreseeable given the  
2 known high frequency of cyberattacks and data breaches in the healthcare industry.  
3

4 214. Defendant has full knowledge of the sensitivity of the Private  
5 Information and the types of harm that Plaintiff and the Class could and would suffer  
6 if the Private Information were wrongfully disclosed.  
7

8 215. Plaintiff and the Class were the foreseeable and probable victims of any  
9 inadequate security practices and procedures. Defendant knew or should have  
10 known of the inherent risks in collecting and storing the Private Information of  
11 Plaintiff and the Class, the critical importance of providing adequate security of that  
12 Private Information, and the necessity for encrypting Private Information stored on  
13 Defendant's systems or transmitted through third party systems.  
14  
15

16 216. It was therefore foreseeable that the failure to adequately safeguard  
17 Class Members' Private Information would result in one or more types of injuries to  
18 Class Members.  
19

20 217. Plaintiff and the Class had no ability to protect their Private Information  
21 that was in, and possibly remains in, Defendant's possession.  
22

23 218. Defendant was in a position to protect against the harm suffered by  
24 Plaintiff and the Class as a result of the Data Breach.

25 219. Defendant's duty extended to protecting Plaintiff and the Class from  
26 the risk of foreseeable criminal conduct of third parties, which has been recognized  
27  
28

1 in situations where the actor's own conduct or misconduct exposes another to the  
2 risk or defeats protections put in place to guard against the risk, or where the parties  
3 are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous  
4 courts and legislatures have also recognized the existence of a specific duty to  
5 reasonably safeguard personal information.  
6

7  
8 220. Defendant has admitted that the Private Information of Plaintiff and the  
9 Class was wrongfully lost and disclosed to unauthorized third persons as a result of  
10 the Data Breach.  
11

12 221. But for Defendant's wrongful and negligent breach of duties owed to  
13 Plaintiff and the Class, the Private Information of Plaintiff and the Class would not  
14 have been compromised.  
15

16 222. There is a close causal connection between Defendant's failure to  
17 implement security measures to protect the Private Information of Plaintiff and the  
18 Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class.  
19 The Private Information of Plaintiff and the Class was lost and accessed as the  
20 proximate result of Defendant's failure to exercise reasonable care in safeguarding  
21 such Private Information by adopting, implementing, and maintaining appropriate  
22 security measures.  
23  
24

25 223. As a direct and proximate result of Defendant's negligence, Plaintiff  
26 and the Class have suffered and will suffer injury, including but not limited to: (i)  
27  
28

1 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished  
2 value of Private Information; (iv) lost time and opportunity costs associated with  
3 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit  
4 of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the  
5 actual consequences of the Data Breach; (vii) actual misuse of the compromised data  
6 consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private  
7 Information being disseminated on the dark web, according to Experian and Credit  
8 Karma; (ix) statutory damages; (x) nominal damages; and (xi) the continued and  
9 certainly increased risk to their Private Information, which: (a) remains unencrypted  
10 and available for unauthorized third parties to access and abuse; and (b) remains  
11 backed up in Defendant's possession and is subject to further unauthorized  
12 disclosures so long as Defendant fails to undertake appropriate and adequate  
13 measures to protect the Private Information.

14  
15 224. Additionally, as a direct and proximate result of Defendant's  
16 negligence, Plaintiff and the Class have suffered and will suffer the continued risks  
17 of exposure of their Private Information, which remain in Defendant's possession  
18 and is subject to further unauthorized disclosures so long as Defendant fails to  
19 undertake appropriate and adequate measures to protect the Private Information in  
20 its continued possession.  
21  
22  
23  
24  
25  
26  
27  
28

1        225. Plaintiff and Class Members are entitled to compensatory and  
2 consequential damages suffered as a result of the Data Breach.

3  
4        226. Plaintiff and Class Members are also entitled to injunctive relief  
5 requiring Defendant to (i) strengthen its data security systems and monitoring  
6 procedures; (ii) submit to future annual audits of those systems and monitoring  
7 procedures; and (iii) continue to provide adequate credit monitoring to all Class  
8 Members.  
9

10  
11                    **COUNT II**  
12                    **Breach Of Implied Contract**  
13                    **(On Behalf of Plaintiff and the Class)**

14        227. Plaintiff re-alleges and incorporates by reference all preceding  
15 allegations, as if fully set forth herein.

16        228. Plaintiff and Class Members were required deliver their Private  
17 Information to Defendant as part of the process of obtaining healthcare services  
18 provided by Defendant. Plaintiffs and Class Members paid money, or money was  
19 paid on their behalf, to Defendant in exchange for healthcare services.  
20

21        229. Defendant solicited, offered, and invited Class Members to provide  
22 their Private Information as part of Defendant's regular business practices. Plaintiffs  
23 and Class Members accepted Defendant's offers and provided their Private  
24 Information to Defendant.  
25  
26  
27  
28

1           230. Defendant accepted possession of Plaintiffs' and Class Members'  
2 Private Information for the purpose of providing services to Plaintiffs and Class  
3 Members.  
4

5           231. Plaintiff and the Class entrusted their Private Information to Defendant.  
6 In so doing, Plaintiff and the Class entered into implied contracts with Defendant by  
7 which Defendant agreed to safeguard and protect such information, to keep such  
8 information secure and confidential, and to timely and accurately notify Plaintiff and  
9 the Class if their data had been breached and compromised or stolen.  
10

11           232. In entering into such implied contracts, Plaintiff and Class Members  
12 reasonably believed and expected that Defendant's data security practices complied  
13 with relevant laws and regulations (including HIPAA and FTC guidelines on data  
14 security) and were consistent with industry standards.  
15  
16

17           233. Implicit in the agreement between Plaintiff and Class Members and the  
18 Defendant to provide Private Information, was the latter's obligation to: (a) use such  
19 Private Information for business purposes only, (b) take reasonable steps to  
20 safeguard that Private Information, (c) prevent unauthorized disclosures of the  
21 Private Information, (d) provide Plaintiff and Class Members with prompt and  
22 sufficient notice of any and all unauthorized access and/or theft of their Private  
23 Information, (e) reasonably safeguard and protect the Private Information of Plaintiff  
24 and Class Members from unauthorized disclosure or uses, (f) retain the Private  
25  
26  
27  
28

1 Information only under conditions that kept such information secure and  
2 confidential.

3  
4 234. The mutual understanding and intent of Plaintiff and Class Members on  
5 the one hand, and Defendant, on the other, is demonstrated by their conduct and  
6 course of dealing.

7  
8 235. On information and belief, at all relevant times Defendant promulgated,  
9 adopted, and implemented written privacy policies whereby it expressly promised  
10 Plaintiff and Class Members that it would only disclose Private Information under  
11 certain circumstances, none of which relate to the Data Breach.

12  
13 236. On information and belief, Defendant further promised to comply with  
14 industry standards and to make sure that Plaintiff's and Class Members' Private  
15 Information would remain protected.

16  
17 237. Plaintiff and Class Members paid money to Defendant with the  
18 reasonable belief and expectation that Defendant would use part of its earnings to  
19 obtain adequate data security. Defendant failed to do so.

20  
21 238. Plaintiff and Class Members would not have entrusted their Private  
22 Information to Defendant in the absence of the implied contract between them and  
23 Defendant to keep their information reasonably secure.

24  
25 239. Plaintiff and Class Members would not have entrusted their Private  
26 Information to Defendant in the absence of their implied promise to monitor their  
27



1 computer systems and networks to ensure that it adopted reasonable data security  
2 measures.

3  
4 240. Every contract in this State has an implied covenant of good faith and  
5 fair dealing, which is an independent duty and may be breached even when there is  
6 no breach of a contract's actual and/or express terms.

7  
8 241. Plaintiff and Class Members fully and adequately performed their  
9 obligations under the implied contracts with Defendant.

10 242. Defendant breached the implied contracts it made with Plaintiff and the  
11 Class by failing to safeguard and protect their personal information, by failing to  
12 delete the information of Plaintiff and the Class once the relationship ended, and by  
13 failing to provide accurate notice to them that personal information was  
14 compromised as a result of the Data Breach.

15  
16 243. Defendant breached the implied covenant of good faith and fair dealing  
17 by failing to maintain adequate computer systems and data security practices to  
18 safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff  
19 and Class Members and continued acceptance of PII and storage of other personal  
20 information after Defendant knew, or should have known, of the security  
21 vulnerabilities of the systems that were exploited in the Data Breach.

22  
23 244. As a direct and proximate result of Defendant's breach of the implied  
24 contracts, Plaintiff and Class Members sustained damages, including, but not limited  
25  
26  
27  
28

1 to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or  
2 diminished value of Private Information; (iv) lost time and opportunity costs  
3 associated with attempting to mitigate the actual consequences of the Data Breach;  
4 (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with  
5 attempting to mitigate the actual consequences of the Data Breach; (vii) actual  
6 misuse of the compromised data consisting of an increase in spam calls, texts, and/or  
7 emails; (viii) Plaintiff's Private Information being disseminated on the dark web,  
8 according to Experian and Credit Karma; (ix) statutory damages; (x) nominal  
9 damages; and (xi) the continued and certainly increased risk to their Private  
10 Information, which: (a) remains unencrypted and available for unauthorized third  
11 parties to access and abuse; and (b) remains backed up in Defendant's possession  
12 and is subject to further unauthorized disclosures so long as Defendant fails to  
13 undertake appropriate and adequate measures to protect the Private Information.  
14  
15

16 245. Plaintiff and Class Members are entitled to compensatory,  
17 consequential, and nominal damages suffered as a result of the Data Breach.  
18

19 246. Plaintiff and Class Members are also entitled to injunctive relief  
20 requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring  
21 procedures; (ii) submit to future annual audits of those systems and monitoring  
22 procedures; and (iii) immediately provide adequate credit monitoring to all Class  
23 Members.  
24  
25  
26  
27  
28

**COUNT III**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

247. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

248. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

249. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its agents for healthcare services and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the healthcare services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

250. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

251. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

1           252. Defendant acquired the Private Information through inequitable record  
2 retention as it failed to investigate and/or disclose the inadequate data security  
3 practices previously alleged.  
4

5           253. If Plaintiff and Class Members had known that Defendant would not  
6 use adequate data security practices, procedures, and protocols to adequately  
7 monitor, supervise, and secure their Private Information, they would have entrusted  
8 their Private Information at Defendant or obtained healthcare services at Defendant.  
9

10           254. Plaintiff and Class Members have no adequate remedy at law.  
11

12           255. Under the circumstances, it would be unjust for Defendant to be  
13 permitted to retain any of the benefits that Plaintiff and Class Members conferred  
14 upon it.  
15

16           256. As a direct and proximate result of Defendant's conduct, Plaintiff and  
17 Class Members have suffered and will suffer injury, including but not limited to: (i)  
18 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished  
19 value of Private Information; (iv) lost time and opportunity costs associated with  
20 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit  
21 of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the  
22 actual consequences of the Data Breach; (vii) actual misuse of the compromised data  
23 consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private  
24 Information being disseminated on the dark web, according to Experian and Credit  
25  
26  
27  
28

1 Karma; (ix) statutory damages; (x) nominal damages; and (xi) the continued and  
2 certainly increased risk to their Private Information, which: (a) remains unencrypted  
3 and available for unauthorized third parties to access and abuse; and (b) remains  
4 backed up in Defendant's possession and is subject to further unauthorized  
5 disclosures so long as Defendant fails to undertake appropriate and adequate  
6 measures to protect the Private Information.  
7

8  
9 257. Plaintiff and Class Members are entitled to full refunds, restitution,  
10 and/or damages from Defendant and/or an order proportionally disgorging all  
11 profits, benefits, and other compensation obtained by Defendant from its wrongful  
12 conduct. This can be accomplished by establishing a constructive trust from which  
13 the Plaintiff and Class Members may seek restitution or compensation.  
14

15  
16 258. Plaintiff and Class Members may not have an adequate remedy at law  
17 against Defendant, and accordingly, they plead this claim for unjust enrichment in  
18 addition to, or in the alternative to, other claims pleaded herein.  
19

20 **COUNT IV**  
21 **Violation of the California Unfair Competition Law,**  
22 **Cal. Bus. & Prof. Code §17200 *et seq.***  
**(On Behalf of Plaintiff and the Class)**

23 259. Plaintiff re-alleges and incorporates by reference all preceding  
24 allegations, as if fully set forth herein.  
25

26 260. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.  
27  
28

1           261. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”) by  
2 engaging in unlawful, unfair, and deceptive business acts and practices.  
3

4           262. Defendant’s “unfair” acts and practices include:

5           a. Defendant failed to implement and maintain reasonable security  
6 measures to protect Plaintiff’s and Class Members’ personal  
7 information from unauthorized disclosure, release, data breaches, and  
8 theft, which was a direct and proximate cause of the Data Breach.

9           Defendant failed to identify foreseeable security risks, remediate  
10 identified security risks, and adequately improve security following  
11 previous cybersecurity incidents and known coding vulnerabilities in  
12 the industry;  
13

14           b. Defendant’s failure to implement and maintain reasonable security  
15 measures also was contrary to legislatively-declared public policy that  
16 seeks to protect consumers’ data and ensure that entities that are trusted  
17 with it use appropriate security measures. These policies are reflected  
18 in laws, including the FTC Act (15 U.S.C. § 45), HIPAA, California’s  
19 Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and  
20 California’s Consumer Privacy Act (Cal. Civ. Code § 1798.150);  
21

22           c. Defendant’s failure to implement and maintain reasonable security  
23 measures also led to substantial consumer injuries, as described above,  
24  
25  
26  
27  
28

1 that are not outweighed by any countervailing benefits to consumers or  
2 competition. Moreover, because consumers could not know of  
3 Defendant's inadequate security, consumers could not have reasonably  
4 avoided the harms that Defendant caused; and  
5

- 6 d. Engaging in unlawful business practices by violating Cal. Civ. Code §  
7 1798.82.  
8

9 263. Defendant has engaged in "unlawful" business practices by violating  
10 multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.  
11

12 264. Defendant's unlawful, unfair, and deceptive acts and practices include:

- 13 a. Failing to implement and maintain reasonable security and privacy  
14 measures to protect Plaintiff's and Class Members' personal  
15 information, which was a direct and proximate cause of the Data  
16 Breach;  
17  
18 b. Failing to identify foreseeable security and privacy risks, remediate  
19 identified security and privacy risks, which was a direct and proximate  
20 cause of the Data Breach;  
21  
22 c. Failing to comply with common law and statutory duties pertaining to  
23 the security and privacy of Plaintiff's and Class Members' personal  
24 information, including duties imposed by the FTC Act, 15 U.S.C. § 45,  
25 which was a direct and proximate cause of the Data Breach;  
26  
27  
28

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

265. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

266. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive



1 acts, practices, and omissions alleged herein, time and expenses related to  
2 monitoring their financial accounts for fraudulent activity, an increased, imminent  
3 risk of fraud and identity theft, and loss of value of their personal information.  
4

5 267. Defendant's violations were, and are, willful, deceptive, unfair, and  
6 unconscionable.  
7

8 268. Plaintiff and Class Members have lost money and property as a result  
9 of Defendant's conduct in violation of the UCL, as stated herein and above.  
10

11 269. By deceptively storing, collecting, and disclosing their personal  
12 information, Defendant has taken money or property from Plaintiff and Class  
13 Members.  
14

15 270. Defendant acted intentionally, knowingly, and maliciously to violate  
16 California's Unfair Competition Law, and recklessly disregarded Plaintiff's and  
17 Class Members' rights.  
18

19 271. Plaintiff and Class Members seek all monetary and nonmonetary relief  
20 allowed by law, including restitution of all profits stemming from Defendant's  
21 unfair, unlawful, and fraudulent business practices or use of their personal  
22 information; declaratory relief; reasonable attorneys' fees and costs under California  
23 Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable  
24 relief, including public injunctive relief.  
25  
26  
27  
28

**COUNT V**

**Violation of the California Consumer Privacy Act,  
Cal. Civ. Code §§ 1798.100 et seq., § 1798.150(a)  
(On Behalf of Plaintiff and the California Subclass)**

272. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the “Class” for the purposes of this count).

273. The California Consumer Privacy Act (“CCPA”), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

274. Defendant is a “business” under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of \$25 million.

1           275. Plaintiff and Class Members are covered “consumers” under §  
2 1798.140(g) in that they are natural persons who are California residents.

3  
4           276. The personal information of Plaintiff and the Class Members at issue in  
5 this lawsuit constitutes “personal information” under § 1798.150(a) and 1798.81.5,  
6 in that the personal information Defendant collects and which was impacted by the  
7 cybersecurity attack includes an individual’s first name or first initial and the  
8 individual’s last name in combination with one or more of the following data  
9 elements, with either the name or the data elements not encrypted or redacted: (i)  
10 Social Security number; (ii) Driver’s license number, California identification card  
11 number, tax identification number, passport number, military identification number,  
12 or other unique identification number issued on a government document commonly  
13 used to verify the identity of a specific individual; (iii) account number or credit or  
14 debit card number, in combination with any required security code, access code, or  
15 password that would permit access to an individual’s financial account; (iv) medical  
16 information; (v) health insurance information; (vi) unique biometric data generated  
17 from measurements or technical analysis of human body characteristics, such as a  
18 fingerprint, retina, or iris image, used to authenticate a specific individual.  
19  
20  
21  
22  
23

24           277. Defendant knew or should have known that its computer systems and  
25 data security practices were inadequate to safeguard the Class Members’ personal  
26 information and that the risk of a data breach or theft was highly likely. Defendant  
27  
28

1 failed to implement and maintain reasonable security procedures and practices  
2 appropriate to the nature of the information to protect the personal information of  
3 Plaintiff and the Class Members. Specifically, Defendant subjected Plaintiff's and  
4 the Class Members' nonencrypted and nonredacted personal information to an  
5 unauthorized access and exfiltration, theft, or disclosure as a result of the  
6 Defendant's violation of the duty to implement and maintain reasonable security  
7 procedures and practices appropriate to the nature of the information, as described  
8 herein.  
9  
10

11  
12 278. As a direct and proximate result of Defendant's violation of its duty,  
13 the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class  
14 Members' personal information included exfiltration, theft, or disclosure through  
15 Defendant's servers, systems, and website, and/or the dark web, where hackers  
16 further disclosed the personal identifying information alleged herein.  
17

18  
19 279. As a direct and proximate result of Defendant's acts, Plaintiff and the  
20 Class Members were injured and lost money or property, including but not limited  
21 to the loss of Plaintiff's and Class Members' legally protected interest in the  
22 confidentiality and privacy of their personal information, stress, fear, and anxiety,  
23 nominal damages, and additional losses described above.  
24  
25  
26  
27  
28

1       280. Section 1798.150(b) specifically provides that “[n]o [prefiling] notice  
2 shall be required prior to an individual consumer initiating an action solely for actual  
3 pecuniary damages.”  
4

5       281. On April 9, 2024, Plaintiff’s counsel sent a CCPA notice letter to  
6 Defendant’s registered service agents via certified mail. If Defendant does not cure  
7 the effects of the Data Breach, which would require retrieving the Private  
8 Information and securing the Private Information from continuing and future use,  
9 within 30 days of delivery of such CCPA notice letter (which Plaintiff believes any  
10 such cure is not possible under these facts and circumstances), Plaintiff shall seek  
11 actual damages and statutory damages of no less than \$100 and up to \$750 per  
12 customer record subject to the Data Breach on behalf of the California Subclass as  
13 authorized by the CCPA.  
14  
15  
16

17       282. Accordingly, Plaintiff and the Class Members by way of this complaint  
18 seek actual pecuniary damages suffered as a result of Defendant’s violations  
19 described herein.  
20

21                                   **COUNT VI**  
22                                   **Violation of the California Customer Records Act,**  
23                                   **Cal. Civ. Code §§ 1798.80 *et seq.***  
24                                   **(On Behalf of Plaintiff and the California Subclass)**

25       283. Plaintiff re-alleges and incorporates by reference all preceding  
26 allegations, as if fully set forth herein, and brings this claim on behalf of herself and  
27 the California Subclass (the “Class” for the purposes of this count).  
28

1       284. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the  
2 Legislature to ensure that personal information about California residents is  
3 protected. To that end, the purpose of this section is to encourage businesses that  
4 own, license, or maintain personal information about Californians to provide  
5 reasonable security for that information.”  
6

7  
8       285. Section 1798.81.5(b) further states that: “[a] business that owns,  
9 licenses, or maintains personal information about a California resident shall  
10 implement and maintain reasonable security procedures and practices appropriate to  
11 the nature of the information, to protect the personal information from unauthorized  
12 access, destruction, use, modification, or disclosure.”  
13

14  
15       286. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a  
16 violation of this title may institute a civil action to recover damages.” Section  
17 1798.84(e) further provides that “[a]ny business that violates, proposes to violate, or  
18 has violated this title may be enjoined.”  
19

20       287. Plaintiff and the Class Members are “customers” within the meaning of  
21 Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided  
22 personal information to Defendant for the purpose of obtaining a product and/or  
23 service from Defendant.  
24

25       288. The personal information of Plaintiff and the Class Members at issue in  
26 this lawsuit constitutes “personal information” under § 1798.81.5(d)(1) in that the  
27  
28

1 personal information Defendant collects and which was impacted by the  
2 cybersecurity attack includes an individual's first name or first initial and the  
3 individual's last name in combination with one or more of the following data  
4 elements, with either the name or the data elements not encrypted or redacted: (i)  
5 Social Security number; (ii) Driver's license number, California identification card  
6 number, tax identification number, passport number, military identification number,  
7 or other unique identification number issued on a government document commonly  
8 used to verify the identity of a specific individual; (iii) account number or credit or  
9 debit card number, in combination with any required security code, access code, or  
10 password that would permit access to an individual's financial account; (iv) medical  
11 information; (v) health insurance information; (vi) unique biometric data generated  
12 from measurements or technical analysis of human body characteristics, such as a  
13 fingerprint, retina, or iris image, used to authenticate a specific individual.  
14  
15  
16  
17  
18

19 289. Defendant knew or should have known that its computer systems and  
20 data security practices were inadequate to safeguard the Plaintiff's and Class  
21 Members' personal information and that the risk of a data breach or theft was highly  
22 likely. Defendant failed to implement and maintain reasonable security procedures  
23 and practices appropriate to the nature of the information to protect the personal  
24 information of Plaintiff and the Class Members. Specifically, Defendant failed to  
25 implement and maintain reasonable security procedures and practices appropriate to  
26  
27  
28

1 the nature of the information, to protect the personal information of Plaintiff and the  
2 Class Members from unauthorized access, destruction, use, modification, or  
3 disclosure. Defendant further subjected Plaintiff's and the Class Members'  
4 nonencrypted and nonredacted personal information to an unauthorized access and  
5 exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to  
6 implement and maintain reasonable security procedures and practices appropriate to  
7 the nature of the information, as described herein.  
8

9  
10 290. As a direct and proximate result of Defendant's violation of its duty,  
11 the unauthorized access, destruction, use, modification, or disclosure of the personal  
12 information of Plaintiff and the Class Members included hackers' access to,  
13 removal, deletion, destruction, use, modification, disabling, disclosure and/or  
14 conversion of the personal information of Plaintiff and the Class Members by the  
15 cyber attackers and/or additional unauthorized third parties to whom those  
16 cybercriminals sold and/or otherwise transmitted the information.  
17  
18

19  
20 291. As a direct and proximate result of Defendant's acts or omissions,  
21 Plaintiff and the Class Members were injured and lost money or property including,  
22 but not limited to, the loss of Plaintiff's and the Class Members' legally protected  
23 interest in the confidentiality and privacy of their personal information, nominal  
24 damages, and additional losses described above. Plaintiff seeks compensatory  
25 damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).  
26  
27  
28



1           292. Moreover, the California Customer Records Act further provides: “A  
2 person or business that maintains computerized data that includes personal  
3 information that the person or business does not own shall notify the owner or  
4 licensee of the information of the breach of the security of the data immediately  
5 following discovery, if the personal information was, or is reasonably believed to  
6 have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82.  
7

9           293. Any person or business that is required to issue a security breach  
10 notification under the CRA must meet the following requirements under  
11 §1798.82(d):  
12

- 13           a. The name and contact information of the reporting person or business  
14           subject to this section;
  - 15           b. A list of the types of personal information that were or are reasonably  
16           believed to have been the subject of a breach;
  - 17           c. If the information is possible to determine at the time the notice is  
18           provided, then any of the following:
    - 19                   i. the date of the breach,
    - 20                   ii. the estimated date of the breach, or
    - 21                   iii. the date range within which the breach occurred. The  
22                   notification shall also include the date of the notice;
- 23  
24  
25  
26  
27  
28

- 1 d. Whether notification was delayed as a result of a law enforcement  
2 investigation, if that information is possible to determine at the time the  
3 notice is provided;  
4
- 5 e. A general description of the breach incident, if that information is  
6 possible to determine at the time the notice is provided;  
7
- 8 f. The toll-free telephone numbers and addresses of the major credit  
9 reporting agencies if the breach exposed a social security number or a  
10 driver's license or California identification card number;  
11
- 12 g. If the person or business providing the notification was the source of  
13 the breach, an offer to provide appropriate identity theft prevention and  
14 mitigation services, if any, shall be provided at no cost to the affected  
15 person for not less than 12 months along with all information necessary  
16 to take advantage of the offer to any person whose information was or  
17 may have been breached if the breach exposed or may have exposed  
18 personal information.  
19  
20

21 294. Defendant failed to provide the legally compliant notice under §  
22 1798.82(d) to Plaintiff and members of the Class. On information and belief, to date,  
23 Defendant has not sent written notice of the data breach to all impacted individuals.  
24 As a result, Defendant has violated § 1798.82 by not providing legally compliant  
25 and timely notice to all Class Members. Because not all members of the class have  
26  
27  
28

1 been notified of the breach, members could have taken action to protect their  
2 personal information, but were unable to do so because they were not timely notified  
3 of the breach.  
4

5 295. On information and belief, many Class Members affected by the breach  
6 have not received any notice at all from Defendant in violation of Section  
7 1798.82(d).  
8

9 296. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and  
10 Class Members suffered incrementally increased damages separate and distinct from  
11 those simply caused by the breaches themselves.  
12

13 297. As a direct consequence of the actions as identified above, Plaintiff and  
14 Class Members incurred additional losses and suffered further harm to their privacy,  
15 including but not limited to economic loss, the loss of control over the use of their  
16 identity, increased stress, fear, and anxiety, harm to their constitutional right to  
17 privacy, lost time dedicated to the investigation of the breach and effort to cure any  
18 resulting harm, the need for future expenses and time dedicated to the recovery and  
19 protection of further loss, and privacy injuries associated with having their sensitive  
20 personal, financial, and payroll information disclosed, that they would not have  
21 otherwise incurred, and are entitled to recover compensatory damages according to  
22 proof pursuant to § 1798.84(b).  
23  
24  
25  
26  
27  
28

**COUNT VII**

**Violation of the California Confidentiality of Medical Information Act,  
Cal. Civ. Code § 56, *et seq.*  
(On Behalf of Plaintiff and the California Subclass)**

298. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the “Class” for the purposes of this count).

299. Defendant is “a provider of health care,” as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

300. At all relevant times, Defendant was a health care provider because they had the “purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual.”

301. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient’s authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

302. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first

1 obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245,  
2 56.26, 56.35, and 56.104.

3  
4 303. Defendant is a person/entity licensed under California under  
5 California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code §  
6 4000, *et seq.*

7  
8 304. Plaintiff and Class Members are "patients" as defined in CMIA, Cal.  
9 Civ. Code §56.05(k) ("Patient" means any natural person, whether or not still living,  
10 who received health care services from a provider of health care and to whom  
11 medical information pertains."). Furthermore, Plaintiff and Class Members, as  
12 patients and customers of Defendant, had their individually identifiable "medical  
13 information," within the meaning of Civil Code § 56.05(j), created, maintained,  
14 preserved, and stored on Defendant's computer network, and were patients on or  
15 before the date of the Data Breach.  
16  
17

18 305. Defendant disclosed "medical information," as defined in CMIA, Cal.  
19 Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in  
20 violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized  
21 individuals in the Data Breach resulted from the affirmative actions of Defendant's  
22 employees, which allowed the hackers to see and obtain Plaintiff's and Class  
23 Members' medical information.  
24  
25  
26  
27  
28

1           306. Defendant negligently created, maintained, preserved, stored, and then  
2 exposed Plaintiff's and Class Members' individually identifiable "medical  
3 information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's  
4 and California Class members' names, addresses, medical information, and health  
5 insurance information, that alone or in combination with other publicly available  
6 information, reveals their identities. Specifically, Defendant knowingly allowed and  
7 affirmatively acted in a manner that allowed unauthorized parties to access,  
8 exfiltrate, and actually view Plaintiff's and Class Members' confidential Private  
9 Information.  
10  
11  
12

13           307. Defendant's negligence resulted in the release of individually  
14 identifiable medical information pertaining to Plaintiff and Class Members to  
15 unauthorized persons and the breach of the confidentiality of that information.  
16 Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or  
17 dispose of Plaintiff's and Class Members' medical information in a manner that  
18 preserved the confidentiality of the information contained therein, in violation of  
19 Cal. Civ. Code §§ 56.06 and 56.101(a).  
20  
21  
22

23           308. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which  
24 prohibit the negligent creation, maintenance, preservation, storage, abandonment,  
25 destruction, or disposal of confidential personal medical information.  
26  
27  
28

1           309. Plaintiff's and Class Members' medical information was accessed and  
2 actually viewed by hackers in the Data Breach.

3  
4           310. Plaintiff's and Class Members' medical information that was the  
5 subject of the Data Breach included "electronic medical records" or "electronic  
6 health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. §  
7 17921(5).  
8

9           311. Defendant's computer systems did not protect and preserve the  
10 integrity of electronic medical information in violation of Cal. Civ. Code §  
11 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted  
12 wrongful actions, inaction, omissions, and want of ordinary care that directly and  
13 proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the  
14 Class Members have suffered (and will continue to suffer) economic damages and  
15 other injury and actual harms including, but not limited to: (i) invasion of privacy;  
16 (ii) theft of their Private Information; (iii) lost or diminished value of Private  
17 Information; (iv) lost time and opportunity costs associated with attempting to  
18 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the  
19 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual  
20 consequences of the Data Breach; (vii) actual misuse of the compromised data  
21 consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private  
22 Information being disseminated on the dark web, according to Experian and Credit  
23  
24  
25  
26  
27  
28

1 Karma; (ix) statutory damages; (x) nominal damages; and (xi) the continued and  
2 certainly increased risk to their Private Information, which: (a) remains unencrypted  
3 and available for unauthorized third parties to access and abuse; and (b) remains  
4 backed up in Defendant's possession and is subject to further unauthorized  
5 disclosures so long as Defendant fails to undertake appropriate and adequate  
6 measures to protect the Private Information.  
7  
8

9 312. As a direct and proximate result of Defendant's wrongful actions,  
10 inaction, omission, and want of ordinary care that directly and proximately caused  
11 the release of Plaintiff's and Class Members' Private Information, Plaintiff and Class  
12 Members' personal medical information was viewed by, released to, and disclosed  
13 to third parties without Plaintiff's and Class Members' written authorization.  
14  
15

16 313. Defendant's negligent failure to maintain, preserve, store, abandon,  
17 destroy, and/or dispose of Plaintiff's and Class Members' medical information in a  
18 manner that preserved the confidentiality of the information contained therein  
19 violated the CMIA.  
20

21 314. Plaintiff and the Class Members were injured and have suffered  
22 damages, as described above, from Defendant's illegal and unauthorized disclosure  
23 and negligent release of their medical information in violation of Cal. Civ. Code  
24 §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36,  
25  
26  
27  
28



1 which allows for actual damages, nominal statutory damages of \$1,000, punitive  
2 damages of \$3,000, injunctive relief, and attorneys' fees, expenses and costs.  
3

4 **PRAYER FOR RELIEF**

5 **WHEREFORE**, Plaintiff, on behalf of herself and Class Members, requests  
6 judgment against Defendant and that the Court grants the following:  
7

- 8 A. For an Order certifying the Classes, and appointing Plaintiff and her  
9 Counsel to represent the Classes;
- 10 B. For equitable relief enjoining Defendant from engaging in the  
11 wrongful conduct complained of herein pertaining to the misuse  
12 and/or disclosure of the Private Information of Plaintiff and Class  
13 Members;  
14
- 15 C. For injunctive relief requested by Plaintiff, including but not limited  
16 to, injunctive and other equitable relief as is necessary to protect the  
17 interests of Plaintiff and Class Members, including but not limited to  
18 an order:  
19
- 20 i. prohibiting Defendant from engaging in the wrongful and unlawful  
21 acts described herein;  
22
- 23 ii. requiring Defendant to protect, including through encryption, all  
24 data collected through the course of its business in accordance with  
25  
26  
27  
28

1 all applicable regulations, industry standards, and federal, state or  
2 local laws;

- 3  
4 iii. requiring Defendant to delete, destroy, and purge the personal  
5 identifying information of Plaintiff and Class Members unless  
6 Defendant can provide to the Court reasonable justification for the  
7 retention and use of such information when weighed against the  
8 privacy interests of Plaintiff and Class Members;  
9  
10 iv. requiring Defendant to provide out-of-pocket expenses associated  
11 with the prevention, detection, and recovery from identity theft, tax  
12 fraud, and/or unauthorized use of their Private Information for  
13 Plaintiff's and Class Members' respective lifetimes;  
14  
15 v. requiring Defendant to implement and maintain a comprehensive  
16 Information Security Program designed to protect the  
17 confidentiality and integrity of the Private Information of Plaintiff  
18 and Class Members;  
19  
20 vi. prohibiting Defendant from maintaining the Private Information of  
21 Plaintiff and Class Members on a cloud-based database;  
22  
23 vii. requiring Defendant to engage independent third-party security  
24 auditors/penetration testers as well as internal security personnel to  
25 conduct testing, including simulated attacks, penetration tests, and  
26  
27  
28

1 audits on Defendant's systems on a periodic basis, and ordering  
2 Defendant to promptly correct any problems or issues detected by  
3 such third-party security auditors;  
4

5 viii. requiring Defendant to engage independent third-party security  
6 auditors and internal personnel to run automated security  
7 monitoring;  
8

9 ix. requiring Defendant to audit, test, and train its security personnel  
10 regarding any new or modified procedures;  
11

12 x. requiring Defendant to segment data by, among other things,  
13 creating firewalls and controls so that if one area of Defendant's  
14 network is compromised, hackers cannot gain access to portions of  
15 Defendant's systems;  
16

17 xi. requiring Defendant to conduct regular database scanning and  
18 securing checks;  
19

20 xii. requiring Defendant to establish an information security training  
21 program that includes at least annual information security training  
22 for all employees, with additional training to be provided as  
23 appropriate based upon the employees' respective responsibilities  
24 with handling personal identifying information, as well as  
25  
26  
27  
28

1 protecting the personal identifying information of Plaintiff and  
2 Class Members;

- 3  
4 xiii. requiring Defendant to routinely and continually conduct internal  
5 training and education, and on an annual basis to inform internal  
6 security personnel how to identify and contain a breach when it  
7 occurs and what to do in response to a breach;  
8  
9 xiv. requiring Defendant to implement a system of tests to assess its  
10 respective employees' knowledge of the education programs  
11 discussed in the preceding subparagraphs, as well as randomly and  
12 periodically testing employees' compliance with Defendant's  
13 policies, programs, and systems for protecting personal identifying  
14 information;  
15  
16 xv. requiring Defendant to implement, maintain, regularly review, and  
17 revise as necessary a threat management program designed to  
18 appropriately monitor Defendant's information networks for  
19 threats, both internal and external, and assess whether monitoring  
20 tools are appropriately configured, tested, and updated;  
21  
22 xvi. requiring Defendant to meaningfully educate all Class Members  
23 about the threats that they face as a result of the loss of their  
24  
25  
26  
27  
28

- 1 confidential personal identifying information to third parties, as  
2 well as the steps affected individuals must take to protect herself;  
3  
4 xvii. requiring Defendant to implement logging and monitoring  
5 programs sufficient to track traffic to and from Defendant's  
6 servers; and  
7  
8 xviii. for a period of 10 years, appointing a qualified and independent  
9 third party assessor to conduct a SOC 2 Type 2 attestation on an  
10 annual basis to evaluate Defendant's compliance with the terms of  
11 the Court's final judgment, to provide such report to the Court and  
12 to counsel for the class, and to report any deficiencies with  
13 compliance of the Court's final judgment;  
14  
15  
16 D. For an award of damages, including actual, nominal, statutory,  
17 consequential, and punitive damages, as allowed by law in an amount  
18 to be determined;  
19  
20 E. For an award of attorneys' fees, costs, and litigation expenses, as  
21 allowed by law;  
22  
23 F. For prejudgment interest on all amounts awarded; and  
24  
25 G. Such other and further relief as this Court may deem just and proper.

26 **JURY TRIAL DEMANDED**

27 Plaintiff hereby demands a trial by jury on all claims so triable.  
28

1  
2 Dated: April 9, 2024

Respectfully Submitted,

3  
4 By: /s/ John J. Nelson

John J. Nelson (SBN 317598)

5 **MILBERG COLEMAN BRYSON**

6 **PHILLIPS GROSSMAN, PLLC**

280 S. Beverly Drive

7 Beverly Hills, CA 90212

8 Telephone: (858) 209-6941

9 Email: jnelson@milberg.com

10 *Attorney for Plaintiff and*  
11 *the Proposed Class*  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28